Ulrich Sieber / Nicolas von zur Mühlen / Tatiana Tropina (eds.)

Access to Telecommunication Data in Criminal Justice

Schriftenreihe des Max-Planck-Instituts für
ausländisches und internationales Strafrecht

Strafrechtliche Forschungsberichte

Herausgegeben von Ulrich Sieber

Band S 156.1

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Access to Telecommunication Data in Criminal Justice

A Comparative Legal Analysis

2nd revised and expanded edition

Ulrich Sieber • Nicolas von zur Mühlen
Tatiana Tropina (eds.)

Volume 1

Duncker & Humblot • Berlin

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten
© 2021 Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.
c/o Max-Planck-Institut für ausländisches und internationales Strafrecht
Günterstalstraße 73, 79100 Freiburg i.Br.
http://www.mpicc.de
Vertrieb in Gemeinschaft mit Duncker & Humblot GmbH, Berlin
http://www.duncker-humblot.de

Umschlagbild: © istock.com/kynny
Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim
Printed in Germany
Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706

ISSN 1860-0093
ISBN 978-3-86113-767-2 (Max-Planck-Institut)
ISBN 978-3-428-18272-5 (Duncker & Humblot)
DOI unter https://doi.org/10.30709/978-3-86113-767-2
CC-Lizenz by-nc-nd/3.0

Preface

Access to telecommunication data is an essential and powerful investigative tool in criminal justice. At the same time, the interception of such data can seriously affect individual privacy. This is true not only with respect to content data but with respect to traffic data as well. The legal instruments and provisions that allow the gathering of these data are primarily the traditional rules on the interception of telecommunication based on the cooperation duties of telecommunication providers. In addition, access to telecommunication data can also be granted by rules on remote forensic software, by search and seizure of – temporarily or permanently – stored data, and (esp. in cases of traffic and subscriber data) by production orders demanding the delivery of stored data.

The rules governing these interception techniques vary considerably among the national legal orders. Differences are found, for example, in the formal requirements for interception orders, in the scope of professional secrecy and privacy protections leading to the exemption from interception, and in the possibilities to access (esp. encrypted) telecommunication data by means of remote forensic software, either to specifically procure telecommunication data or in general. These legal differences are not only most interesting from the perspective of fundamental research in the area of comparative criminal law but also for practical reasons, such as identifying best practices and evaluating the scope of international cooperation.

This publication provides a comparative analysis dealing with the commonalities and differences of these rules on interception and other means of access to telecommunication data. It also includes country reports on the following legal orders on which this comparison is based: Australia, Austria, Belgium, Croatia, the Czech Republic and Slovakia, Estonia, France, Germany, Hungary, Italy, the Netherlands, Poland, Portugal, Spain, Sweden, the Untited Kingdom, and the United States of America. The research undertaken on these countries encompasses not only the law on the books but also the law in action as analyzed in interviews and workshops with specialists in the fields of telecommunication interception and international cooperation in criminal matters. The analysis of law in action also includes Switzerland, in addition to the above-mentioned countries.

The original incentive to conduct this analysis was an expert opinion prepared for the German Central Office for Information Technology in the Security Sector (ZITiS) on international cooperation in the interception of telecommunication. International cooperation in this area based on mutual legal assistance was and still is complicated, slow, and – in practice – rare. For these reasons, the goal of the study

for the ZITiS was to develop legal and technical solutions by means of which telecommunication data could be transmitted from one country to another in real time, by direct transmission, and without violating human rights standards. Since such transmissions are especially problematic due to differences in the laws of the various national orders (esp. professional secrecy and privacy protections), the study also required a specific comparative analysis of these differences. The solutions developed for ZITiS on international cooperation was published in a separate volume (S 157 of this book series) in German.

The wealth of information gathered by this practice-oriented study on international cooperation inspired us to develop our applied research into a general comparative analysis on access to telecommunication data, which is published in this book. In contrast to the above-mentioned study for the ZITiS, this general comparative analysis is written in English and addresses not only questions that arise in the context of mutual legal assistance in interception of content data but rather covers all questions implicated in the context of access to telecommunication data. Thus, the scope of this second study extends beyond traditional interception and includes all types of access to telecommunication data that can be used as functional equivalents to traditional interception. Additionally, it is not limited to the interception of content data but rather covers access to traffic and subscriber data as well. In contrast to the above-mentioned study, this publication contains both the results of the comparative study as well as the underlying country reports. As a consequence, the general analysis on access to telecommunication data presented here not only supports our specific study on legal cooperation in interception but can also serve as a general research tool in support of future studies and practical work.

We would like to thank both the academic authors of the country reports for their most valuable support of this study and the many dedicated practitioners who provided us with comprehensive, detailed information about the concrete situation in their countries in interviews in Brussels, Budapest, Gießen, Lisbon, London, Madrid, Paris, Prague, Rome, Stockholm, Tallinn, Utrecht, Vienna, and Zurich. Above all, we are most grateful to Mr. *Christian Förster* from ZITiS as the appointed project manager, who efficiently organized and made possible these interviews on "the law in action." In addition, sincere thanks are also due to our editing and proofreading teams, especially Ms. *Petra Lehser*, Ms. *Indira Tie*, and Ms. *Anna Riddell* (as external proofreader).

Freiburg, March 2021

Prof. Dr. Dr. h.c. mult. *Ulrich Sieber*
Dr. *Nicolas von zur Mühlen*
Dr. *Tatiana Tropina*

Contents

Part 1 – Introduction: Object, Aims, and Research Methods

Ulrich Sieber
Nicolas von zur Mühlen

Contents

I. Subject

The interception of telecommunication is key in the practice of law enforcement. It has significantly gained in importance over the last few years. In addition to (repressive) measures based on criminal law, all countries also employ (preventive) measures that authorize interception, especially measures of intelligence law.

One of the reasons for this significance of telecommunication interception is the fact that modern communication techniques have been instrumental in recent decades in inducing a profound change in society, commonly termed "information society." By now, digital interconnectivity permeates almost all aspects of life. Technological media have increasingly replaced the direct and personal exchange of information. End user devices such as smart phones, tablets, and smartwatches provide uninterrupted connectivity using an array of communication channels. Communication between information systems, aside from the familiar telecommunication between people, has become ever more important. At present, this is particularly true in the context of the transfer of applications, data processing capabilities, and storage into the cloud, and communication between systems is expected to increase even more in the coming years through the so-called internet of things, which links household appliances, vehicles, sensors, and control systems.

As a result of these technological and social changes, law enforcement agencies are facing a host of challenges, not least because criminal offenders are also users of modern communication technologies. The use of such technologies is particularly significant in crimes planned and executed by offender groups operating mostly in a decentralized and trans-national manner, particularly in the areas of organized crime, terrorism, economic crime, and cybercrime.

In addition, the new risks presented by terrorism, organized crime, economic crime, and cybercrime have made it necessary to prevent these offenses as early in the process of commission as possible, which in turn requires intensified information-gathering prior to the actual commission of a crime. The need for these efforts to gather information before actual harm is caused arises not only in the context of preventive information gathering by police and intelligence services but also in criminal investigations. The reason is that recently enacted precursor offenses increasingly criminalize preparatory acts – acts that, for the most part, are objectively value neutral and are criminalized mainly because the offender has certain offenses in mind or the requisite knowledge of such offenses. This type of investigation conducted prior to the occurrence of any actual harm and for the purpose of proving criminal intent and knowledge may be accomplished primarily by means of telecommunication interception.

Currently, telecommunication interception is *functionally* linked to new technological and legal problems. *Technological* problems arise primarily from the encryption of communication, from the wealth of telecommunication service providers used, and from the huge number of terminal devices, protocols, and applications. These developments generate new *legal* issues and approaches, such as source telecommunication surveillance and the growing number of requirements imposed on service providers. More legal problems arise from the fact that the distinction between access to stored data and access to transmitted data (such as temporarily stored emails) is blurred in the internet. Another question involves the conditions that would permit the authorized interception not only of person-to-person communication but also of communication between persons and machines (such as during interception of the retrieval of websites) and of exchanges of data between technological devices (such as in the internet of things).

These technological and legal problems increase exponentially at the *territorial* level if offenders operate *across borders*. In these cases, the interception of the telecommunication of a suspect who travels abroad becomes even more complicated in terms of law because the authority of investigative agencies to engage in telecommunication interception are limited, in principle, to the national territory; as a rule, any interception of telecommunication systems in a foreign state constitutes a violation of that country's sovereignty. However, the required mutual legal assistance in matters involving foreign countries presents additional legal challenges. The main challenge is due to the fact that different national legal systems have different provisions on telecommunication interception, which may conflict with a transfer of data, for example, in terms of the new legal problems mentioned above or in terms of different definitions of professional secrecy leading to exemption from telecommunication interception. In addition, prosecutors are saddled with more legal and organizational problems: the special, little-known, and complex topic of mutual legal assistance; the ambiguities in the national law of the requested state; and translation issues involved in providing mutual legal assistance. And, above all, the technological difficulties that may arise, for example, if each state involved employs a different system for telecommunication interception, thus creating compatibility issues. These problems are compounded if the interception results need to be transferred not only as "canned" information in data files but in real time over data lines to enable an immediate response on the part of the investigation agencies in the requesting state. For these reasons, national borders within the European Union continue to create major challenges for the efficient interception of transnational telecommunication.

However, these transnational cases of interception create problems not only in terms of the efficiency of criminal justice but also in terms of the protection of the citizens concerned. To take an example: By way of mutual legal assistance, a router's data packets recorded in Germany, which might possibly include communication by a member of the clergy or data from the core area of privacy (which, in

Germany, may neither be surveilled nor evaluated), might be directly transmitted to France (where no such legal privileges exist). Similarly, in England, telecommunication interception may be issued without court order: what if such a request is transmitted to the German authorities by way of mutual legal assistance? If telecommunication interception results are transmitted to a foreign country in real time, the opportunity to engage in the control and selection of transmitted data is even more limited. Any transmission of telecommunication interception results to a foreign country in real time, which is needed for effective investigations, means a further reduction in the ability to control and select the transmitted data.

II. Research Aims

The first aim of this study is to identify, by a comprehensive comparative legal analysis, the concepts employed by various states to manage the technological and legal problems involved in telecommunication interception. Special focus is on specific deficiencies in existing methods of lawful intervention and on the different approaches developed to address specific problems.

By providing a comprehensive overview of the relevant national legislation of various countries, this study also seeks to provide a foundation for additional research projects that address both the functional as well as the territorial limits of criminal law in the context of the issue at hand. A pertinent example is the study entitled *Rechtshilfe in der Telekommunikationsüberwachung* (Mutual legal assistance in telecommunication interception) mentioned in the Preface. Its aim is to generate an effective system of transnational telecommunication interception that provides an appropriate level of protection for the citizens involved and, as such, is compatible with constitutional and human rights guarantees.

An additional goal of this study is to support law enforcement agencies by presenting the various national laws in a way that helps make international cooperation in the context of telecommunication interception more effective. Requests for telecommunication interception can be successful only if the investigating authorities know the pertinent local rules.

III. Research Method

A. Identifying Relevant Provisions

This research study addresses the national *laws of criminal procedure* and the national *laws on telecommunication* of the participating countries, specifically the powers of intervention involving telecommunication interception provided by the

laws of criminal procedure and the specific provisions on the obligations of providers. In most countries, the latter requirements are enacted as special legislation or as ordinances. In order to create a foundation for further projects on issues involving telecommunication interception (in particular, the above-mentioned study entitled *Rechtshilfe in der Telekommunikationsüberwachung*), this study also covers relevant national provisions on mutual legal assistance.

B. Selecting Legal Systems for the Study

The following eight countries were selected to participate in a first stage of the study, which was published in 2016: Belgium, the Czech Republic, France, Germany, the Netherlands, Sweden, Spain, and the United Kingdom. These states are all EU members, and all of them have ratified the Council of Europe Convention on mutual legal assistance. By incorporating German, Nordic, and Roman law legal systems as well as the Common Law system, they reflected the legal diversity in Europe.

In a second stage of the study, the information on the afore-mentioned countries was updated and the following ten countries were added: Australia, Austria, Croatia, Estonia, Hungary, Italy, Poland, Portugal, Switzerland, and the Untited States of America. The selection of the resulting 18 – primarily European – legal orders is based on the fact that the present study was originally designed with respect to a concrete project for improved cooperation in real-time telecommunication interception between European states, as described in the preface. The aim of additionally including Australia and the USA in the second phase of the study was to explore the chances of a later extension of the cooperation model to these common law countries.

For 16 of these 18 countries, we were able to obtain detailed country reports which follow the same structure and which are now published in the present book, along with a shorter special report on the law in the USA and a comparative report.

C. Obtaining Relevant Country Information

1. Issue

The study involves not only multiple legal systems but also numerous aspects of law in these systems, including the pertinent law of criminal procedure and various aspects of constitutional law, telecommunication law, and the law of mutual legal assistance. Additional expertise is required because the aim of this study, which also includes practical objectives, influences not only the analysis of the law on the books but also the law in practice.

Obtaining reliable information on the laws of the participating countries, including the "law in action," led a combination of two methods of data collection: first, country reports by foreign legal scholars who are specialists in telecommunication law or information law, and second, interviews and workshops with members of the police and the judiciary working in the area of prosecution, in particular in organized crime and mutual legal assistance on telecommunication interception.

2. Country reports

The "law on the books" was analyzed on the basis of the responses to a standard questionnaire provided to experts on telecommunication interception in the aforementioned countries. In order to enable a comparative legal analysis, the reports are all organized according to the same outline.

- The country report Australia was written by *Catherine Smith*, consultant and former assistant secretary at the Attorney-General's Department, Canberra.
- The country report Austria was written by Assoz. Prof. Dr. *Christian Bergauer*, Dr. *Diana Bernreiter*, Dr. *Sebastian Gölly*, and Prof. Dr. *Gabriele Schmölzer*, University of Graz.
- The country report Belgium was written by *Gertjan Boulet* and Prof. Dr. *Paul De Hert*, Vrije Universiteit Brussel and Tilburg.
- The country report Czech Republic was prepared under the leadership of doc. JUDr. *Radim Polčák*, Ph.D., University of Brno. This report includes a comparative presentation of the law of Slovakia, which is very similar to the law of the Czech Republic.
- The country report Estonia was written by *Aare Kruuser*, Tallinn University.
- The country report France was written by Dr. *Estelle De Marco*, Inthemis, Montpellier.
- The German country report on telecommunication law was prepared under the leadership of Prof. Dr. Dr. h.c. mult. *Ulrich Sieber* and Dr. *Nicolas von zur Mühlen* by staff members Dr. *Benjamin Vogel*, LL.M. (Cantab.)*, Patrick Köppen*, and *Thomas Wahl* of the Max Planck Institute for Foreign and International Criminal Law.
- The country report Hungary was written by Asst. Prof. *Katalin Parti*, Ph.D., Virginia Tech, Blacksburg, VA.
- The country report Italy was written by Asst. Prof. Dr. *Roberto Flor*, University of Verona, and Assoc. Prof. Dr. *Stefano Marcolini*, University of Varese.
- The country report Croatia was written by doc. dr. sc. *Marko Jurić* (University of Zagreb) and Assoc. Prof. Dr. Dr. h.c. *Sunčana Roksandić* (University of Zagreb).
- The country report the Netherlands was written by *Niels van Buiten,* former prosecutor, Netherlands Public Prosecution Service.
- The country report Poland was written by dr hab. *Sławomir Steinborn*, University of Gdańsk, and Assoc. Prof. Dr. *Stanisław Tosza*, University of Luxembourg.

- The country report Portugal was written by *Pedro Verdelho*, General Prosecutor's Office of Lisbon.
- The country report Spain was written by Prof. Dr. Dr. h.c. *Lorena Bachmaier Winter*, Complutense University of Madrid.
- The country report Sweden was written by Prof. *Iain Cameron*, University of Uppsala.
- The country report United Kingdom was written by *Elif Mendos Kuskonmaz*, Ph.D. (as successor to the report by Prof. *Ian Walden*, Ph.D. in the first edition of this book), Portsmouth.
- A special country report on the legal development in the United States of America was written by Prof. *Joseph J. Schwerha IV*, California University of Pennsylvania.

3. Workshops with legal practitioners

Primarily in order to incorporate law in action, a one-day workshop was organized in 14 of the participating legal systems. The main goal of these workshops was to provide an opportunity for questions and discussions on legal and practical issues involving police and judicial practice. Participants in the discussions were investigators and prosecutors experienced in telecommunication interception as well as specialists on mutual legal assistance. The analysis of law in action also includes Switzerland, in addition to the above-mentioned countries.

4. Questionnaires and scope of analysis

Both the country reports and the interviews with practitioners were based on detailed, highly-structured questionnaires. Both questionnaires were designed by Prof. Dr. *Ulrich Sieber* in cooperation with Dr. *Nicolas von zur Mühlen* and can be found in the Appendix, along with the country reports and the summaries of interviews with practitioners.

With regard to the law of criminal procedure, both questionnaires expanded the subject matter over and above the regulatory scope of telecommunication interception to include issues regarding access to stored communication data and additional questions regarding access to computer-stored data (in particular, issues surrounding the distinction between transmitted and stored data). The reasons for this were twofold: First, to leverage the availability of these specialists from academia and legal practice to obtain data for future research on digital investigative measures. Second, the objective for the research issue at hand was to address all types of access to communication data, i.e., both data transmitted and data stored, in order to identify by means of a comprehensive, functional approach any consequences arising from regulations for mutual legal assistance relating to telecommunication interception.

D. Comparative Legal Analysis

The aim of this study is to analyze concepts for the interception of telecommunication. In line with this, a comparative legal analysis was undertaken, based on the information derived from the country reports, to determine where the participating legal systems converge and where they diverge. The resulting findings on common features and differences between national regulations facilitated an assessment, not only in terms of each country under study but also generally and comprehensively, of potential challenges to international cooperation.

The aim of the study determined both subject matter and scope of the comparative legal analysis. Accordingly, the possibilities and limits of telecommunication interception under the rules of criminal procedure and telecommunication law were at the heart of this legal analysis. The comprehensive questionnaires, developed on the basis of a functional approach, made it easy to compare country information. This provided the basis for Dr. *Tatiana Tropina* of the Max Planck Institute for Foreign and International Criminal Law to prepare a comparative legal analysis that focuses on the national law on telecommunication interception (Part 2).

IV. Subsequent Outline

The following part 2 begins with a *comparative* legal outline of the law on criminal procedure and on telecommunication relating to telecommunication interception. The above-mentioned extensive 16 country reports of parallel structure, which served as the foundation for the comparative legal outline, follow in alphabetical order by country. The additional special report on the law of the United States of America follows.

Part 2
Comparative Analysis

Tatiana Tropina

Contents

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Security Services with Powers of Telecommunications Interception

The interception of electronic communications has become one of the major instruments for criminal investigation. At the same time, however, this measure is also being used for the prevention of future dangers and for information gathering by intelligence agencies. While this study analyses the lawful interception of communications in criminal procedure, it is important to understand the role that such interception has for the purpose of criminal investigation and criminal prosecution in different interception regimes – such as interception for intelligence purposes, crime prevention, or to address dangers – and whether there is a separation between them. The following chapter attempts to analyse the entire spectrum of different legal regimes that provide coercive powers for the interception of electronic communications in eighteen countries included in this study, with the aim of embedding the interception of communications for the purpose of criminal justice into the broader context of the national security architecture.

In this chapter and throughout this comparative report, most of the divergencies in the national laws are illustrated by examples when a full comparison of the laws would be too complex or too repetitive in the context of comparative analysis. However, the analysis seeks to provide as much insight into the national legislation as possible by going into detail without losing the focus on comparison.

1. National security architecture

In all eighteen countries included in this study, the interception of communications can be carried out by different authorities under various interception regimes provided for in the legislation of their respective jurisdictions. In most of the states, except the **United Kingdom**, distinct laws govern interception for the purpose of the prosecution and prevention of crime.

Security-related legislation at the national level constitutes a system of different legislative acts on the powers of various authorities tasked with security issues for the purpose of crime prevention and safety of the state. In all of the jurisdictions, this architecture includes police forces and various security entities, such as intelligence agencies, the military, civil defence bodies, and, in some countries, customs authorities.

The structures of security regimes at the national level are usually very complex and are almost incomparable because of the organisational differences and specifics

of national laws establishing and governing their security architectures. Even the police agencies, which exist in every country, may be differently set up, and have complex organisational structures. For example, in **Spain**, the police consist of three different bodies – National Police, Guardia Civil, and municipal police – with only the first two being granted the power to intercept communications. While these two Spanish police forces have a number of exclusive responsibilities for the investigation of certain types of crimes, their domains might overlap, depending on the number of inhabitants in a city or the agency that is first to receive information about a crime.[1] This creates a complex system of application of police regulations in practice. Another illustrative example of a specific regulation is **Sweden**, where two police bodies – national police and security police, which represents internal intelligence services – were separated institutionally, but not legally, in January 2015. The two structures still partially operate under the same legislation and can both intercept communications and share information.[2]

Further differences in the national security architecture arise from the complexity of the national regimes concerning intelligence agencies and other entities responsible for state security. The framework and design of such systems include various agencies at the national level tasked with state security as well as military and civil defence. For example, in **Germany**, the security system includes offices for the protection of the Constitution, established at both the state and the federal levels, and, at the national level, the Federal Intelligence Service (BND) and the Military Counterintelligence Service (MAD).[3] More examples of national security architecture, including detailed information on police and security services as well as the respective legislation regulating them, can be found in the country reports.

2. Powers for the interception of telecommunications

Most of the national reporters indicate that their respective interception regimes include three pillars: preventive police law, repressive criminal procedural law, and state security legislation, all of them providing the framework for the interception of communications. The reports also note that the law of criminal procedure is one of the main regimes regulating interception for the investigation of crime. There are several exceptions to this general model of having three regimes allowing for interception. In the **Czech Republic**, police law does not allow interception for crime prevention. Similarly, in **Croatia**, there is no interception available under preventive police law: police can order interception only in the course of criminal pro-

---

[1] Information obtained at the law enforcement workshop.

[2] Swedish country report, Chapter I.A.2. and information from the Swedish law enforcement workshop.

[3] German country report, Chapter I.A.1.

ceedings.[4] In **Australia**, the interception legislation in general does not allow police to intercept for preventative purposes, except in a very limited number of circumstances related to terrorist activity or hostile activity by a foreign country.[5]

One of the most important issues in this regard is the question of safeguards provided by different regimes allowing for the interception of communications: the level of checks and balances can differ for preventive, repressive, and intelligence purposes. The national reporters from the **Czech Republic** specifically highlight that the law of criminal procedure in their country provides much stricter safeguards for the interception of communications, such as the need for court authorisation, compared to other existing interception regimes.[6] The **Italian** report indicates that the recent amendments to preventive police law allow interception of communications with the authorisation of the prosecutor, not judicial authorisation, with regard to serious crimes.[7] Stricter regulation concerning the level of safeguards can be found in **Germany**, where interception both for the purpose of prevention and for criminal investigations requires a court order. However, German legislation regulating interception carried out by intelligence services does not require judicial authorisation and establishes "mere factual indication" as a prerequisite instead of requiring a certain degree of suspicion,[8] thus providing fewer safeguards for acquiring communications by means of intelligence agencies.

In contrast, **Sweden** has the same requirements for judicial authorisation of interception carried out by intelligence services and law enforcement agencies, but fewer checks and balances for capturing communications for the purpose of crime prevention or for certain types of investigations. Swedish legislation requires both national police and security police (internal intelligence) to obtain judicial approval for interception; however, exceptions to the requirement of court authorisation are granted to the security police based on special legislation on the investigation of particularly dangerous crimes.[9]

3. Responsibility for the technical performance of interception measures

In all of the countries included in this study, the general mode of the interception of communications for the purpose of criminal investigations is to order communications providers to extract data and surrender them to the respective agencies responsible for carrying out the interception. However, different approaches to the

---

4 Croatian country report, Chapter 1.A.2.

5 Australian country report, Chapter 1.A.2.

6 French country report, Chapter I.A.2.b.; Czech country report, Chapter I.A.2.c.

7 Italian country report, Chapter I.A.2.

8 German country report, Chapter I.A.2.c.

9 Swedish country report, Chapter I.A.2.

centralisation of interception lead to divergences in the implementation of this general mode, both technically and functionally, on the national level.

As can be seen from the analysis of the country reports and from information obtained at practical workshops, the bodies responsible for the interception platforms may vary, ranging from designated technical units within the police to special departments within the Ministry of Justice. Furthermore, in addition to carrying out interception with the help of communications service providers, law enforcement agencies can use their own technical tools to carry out the interception or the acquisition of certain types of communications and other data.

Most of the countries, including **Austria**, the **Czech Republic**, **Belgium**, **Hungary**, the **Netherlands**, **Sweden**, **Switzerland**, and the **United Kingdom,** have **centralised** interception platforms either within the police unit or within the Ministry of Justice, which use the equipment installed at the communications providers. **France's** centralised interception platform and its organisational structure underwent a major reform concerning the interception system in 2016, when police supervision of the system was replaced by control of the Ministry of Justice.[10]

In two states – **Germany** and **Spain** – interception is **not centralised**. **Germany**, due to its federal state structure, has a multifaceted network of platforms for the interception of communications in its federal territories. In **Spain**, the system is also complex because there are two police units – Guardia Civil and Policia Nacional – responsible for the interception, each of them having its own platform. There are also several platforms in the territories, such as Catalonia, the Basque Country, and Navarra.

Furthermore, in some countries, like the **Czech Republic**, **Estonia**, **Hungary**, and **Belgium**, law enforcement agencies share the technical platform for interception with intelligence agencies. Yet other jurisdictions, like **Spain**, feature a separation of platforms for different agencies.

The **Netherlands** represent a distinct example in the organisation of its centralised platform, because the country has an additional link in the chain of interception – a Central Information Desk Telecommunications Research, which represents a point of exchange for specific information between law enforcement agencies and communications providers. Before submitting the request for authorisation of a wiretap, investigators must check whether the phone number or IP address is still in use. This information has to be verified with the help of the Central Information Desk Telecommunications Research. Communications providers are obliged to

[10] French country report, Chapter I.A.3. and information from the law enforcement workshop.

refresh identification data every 24 hours, and law enforcement agencies can verify the data with the central desk.[11]

There is a strict separation between responsibility for the technical performance of the interception and actual access to the content of communications. In every country included in this study, it is only law enforcement agencies that gain knowledge of telecommunication content, even if providers are involved in performing the interception.

4. Legitimacy of data transfers between different security agencies

In most of the countries included in this study, except **Sweden** and the **United Kingdom**, intelligence services and other agencies responsible for crime prevention are strictly separated from the bodies dealing with the interception of communications for the purpose of the investigation and prosecution of crime. However, there are still certain frameworks allowing data resulting from interception to be shared between law enforcement and intelligence. Only in the **Netherlands** did the representatives of the law enforcement agencies at the law enforcement workshop indicate that there is almost no possibility for such data sharing in practice. Further analysis shows that, in most jurisdictions, information flows between different interception regimes are possible either because of the lack of strict separation between different regimes, as in **Sweden** and the **United Kingdom**, or because of special legal provisions that allow for information sharing. The conditions for information sharing between different agencies can either be provided for by specific laws, like those in **Belgium** and **Germany**, where legislation establishes a complex set of conditions for such information exchange, or be outlined in generic clauses on cooperation between different national agencies, such as in **Croatia**, the **Czech Republic, France**, and **Spain**, where information sharing is limited.

– *No strict separation concerning information flows*

Naturally, when the intelligence services are not strictly separated, if separated at all, from the agencies dealing with the prevention and investigation of crime, as in **Sweden** and the **United Kingdom,** more flexible rules for information flows between them can be found in the national legal system. In **Sweden**, even after the separation of security services from the police on 1 January 2015, both agencies are still considered to be police organisations: they fall under the same legislation and follow the same rules on how to handle and process information. The Swedish report points out that the Transparency and Secrecy Act 2009 permits information

[11] See Dutch country report, Chapter III.B.5. and *Odinot* et al., Summary – The use of telephone and Internet taps in criminal investigations, 2012, available at https://english.wodc.nl/onderzoeksdatabase/effectiviteit-van-tappen.aspx?cp=45&cs=6798 [last accessed 10/2016].

transfers between different agencies if necessary to carry out their functions, thus making possible the data sharing between different police agencies and the signal intelligence agency (National Defence Radio Establishment).[12] As was shared by law enforcement agency representatives at the workshop in Sweden, in practice, in some type of investigations, e.g. in many terrorist cases, both the police and security services work together and share information throughout the course of an investigation. When data are intercepted for the purpose of crime prevention, however, such sharing is not always possible, because preventive police activity is subject to different legal regulation. Nevertheless, as stated by Swedish law enforcement agencies, permission to use such data can be granted by the prosecutor. Another exception is the participation of the signal intelligence agency in criminal investigations: as the Swedish country report points out, while the Swedish National Defence Radio Establishment can be tasked with assisting in the obtaining intelligence information upon request by the police authorities concerning certain crimes, the inclusion of the signal intelligence agency in the investigation of specific offences is prohibited.[13]

The **United Kingdom** is another country in which the interception of communications can entail cooperation between different agencies, such as security services and police divisions. The law enforcement and intelligence agencies regularly perform joint operations. For example, the GCHQ and the NCA work together in tackling serious and organised crime. Furthermore, different intelligence agencies can have statutory obligations to aid law enforcement. For example, one of the statutory functions of MI5 is to provide assistance to law enforcement agencies in the prevention and detection of serious crime (Section 1(4), the Security Service Act 1989).[14] Therefore, intercepted data might be disclosed to other entities when necessary. The information from the law enforcement workshop, however, revealed that the extracted data are shared only in certain cases and never include the entire interception outcome. Furthermore, the possibility of a law enforcement agency asking an intelligence agency to share information obtained under a bulk interception warrant is restricted by two conditions. First, the law enforcement agency must have exhausted all other means of making progress in the investigation. The second condition is the necessity and proportionality of the request for information sharing.[15]

Furthermore, during the workshop with law enforcement agencies in Switzerland, the Swiss participants indicated that there is no strict separation in their country with regard to the information flows between intelligence agencies and law enforcement. This allows for information exchange between the agencies when intelligence agencies have suspicion of a crime, with the condition that law en-

---

12 Swedish country report, Chapter I.A.4.

13 Ibid.

14 UK country report, Chapter I.A.4.

15 Ibid.

forcement could have obtained the same information via interception, meaning that the requirements for the approval of interception for law enforcement have been met.

– *Strict separation, but information flows are permissible*

In contrast to **Sweden** and the **United Kingdom**, other countries included in this study separate the regimes governing interception carried out by different agencies, thus making information sharing subject to strict rules and procedures. When sharing is possible, it usually falls under one of the two models indicated in this comparative analysis: exchange of the intercepted data either under the specific detailed regulation or under the general rules on information sharing.

Specific regulations on information transfers exist in **Germany** and in **Belgium**. Although police forces and intelligence agencies are separated in **Germany**, the transfer of information gained through the interception of communications is allowed under certain conditions involving the assessment of justification in each individual case of such sharing and the application of the principle of proportionality.[16] Therefore, the possibility to share information depends on which authorities are transferring such information and who the recipient is. For example, although passing on data from law enforcement to preventive police authorities in Germany is, in principle, possible under Section 481 Subsection 1 StPO,[17] information flows in the other direction – from preventive police authorities to law enforcement – are more limited. These data can be shared and used as evidence only if they could have been legally obtained under the law of criminal procedure.[18] Furthermore, the disclosure of data from intelligence to law enforcement is permissible only under the condition of prevention and prosecution of crimes related to state security and a number of other serious crimes.[19] Passing data from an interception measure in the other direction – from law enforcement to intelligence – is also restricted to crimes endangering the security of the state.[20] At the state level, such information transfers are also limited, and the police do not regularly share data with intelligence services.[21]

Even more complex specific frameworks govern data transfers between different agencies in **Belgium**. In principle, the exchange of information is enabled by the Law on the Intelligence and Security Services, which provides the obligation for

---

16 German country report, Chapter I.A.4.

17 Furthermore, some states require threat to life, health, or freedom of persons. For the purpose of investigations into serious crimes, see, e.g. Article 38 Para. 2 of the Bavarian Police Code. See German country report, Chapter I.A.4.a.

18 German country report, Chapter I.A.4.a. referring to Section 161 Subsection 2 StPO.

19 German country report, Chapter I.A.4.b.

20 German country report, Chapter I.A.4.c.

21 Ibid.

the efficiency of mutual cooperation between intelligence and security services, the police, and the judiciary. However, the system for such information exchanges is outlined in different pieces of legislation. Intelligence and security services have a duty to pass on relevant information to the police under the Act of 18 March 2014.[22] Information transfers to the prosecutors are permitted by virtue of Article 29 Code of Criminal Procedure, which requires intelligence and security agencies to inform a public prosecutor immediately if any information about a crime is obtained. The body responsible for such transfers is a special administrative commission, which has the duty to monitor the data collection methods used by the intelligence and security services (SIM commission).[23] Additional cooperation possibilities are outlined in Article 20 Para. 2 of the Act of 30 November 1998 on the Intelligence and Security Services, which states that, upon receiving a request from judicial authorities, intelligence and security services can cooperate with the judicial and administrative authorities, upon their request, and within the limits of a protocol adopted by the relevant ministers. Lastly, the possibility to pass data on to the intelligence agencies also generally falls under the above-mentioned provision on maximally efficient cooperation: police services and judicial authorities can even transfer data at their own initiative.[24] Police and judicial authorities, however, can refuse to provide such requested information to other entities if it might hamper an ongoing investigation and in a number of other circumstances.[25]

Less complex and more general regulation on data sharing exists in **Austria**, **Croatia**, the **Czech Republic**, **France**, and **Spain**, where the possibility for such information transfers is outlined in the generic clauses on cooperation between different national agencies. In **Austria**, data transmission between the agencies is possible under various circumstances that include such purposes as necessity to avert serious crimes.[26] **Croatian** law provides for the obligation of the intelligence agencies to notify the State Attorney's Office if collected intelligence indicates that a criminal act subject to ex officio prosecution is being planned or committed.[27] Similarly, the **Italian** report states that the intelligence staff members have a duty to inform the judicial authority or judicial police about the committed crimes in the same manner as every public official on duty.[28] In **France**, the Internal Security Code provides for the possibility, under certain circumstances, for listed intelligence services or subservices to access certain judicial data processing.[29] In con-

---

[22] Belgian country report, Chapter I.A.4.

[23] Ibid.

[24] Belgian country report, Chapter I.A.4.c. referring to Article 14 Para. 1–2 Act of 30 November 1998 on the Intelligence and Security Services.

[25] Ibid.

[26] Austrian country report, Chapter I.A.4.

[27] Croatian country report, Chapter I.A.4. referring to Article 56 ASIS

[28] Italian country report, Chapter I.A.4.

[29] French country report, Chapter I.A.4.b.

trast, when information sharing goes in the other direction, the French law provides for the duty to pass on data from intelligence agencies to the police under the general regulation (Article 40 Penal Procedure Code),[30] obliging any authority, including intelligence agencies, to pass on information about the crime to the prosecutor.

Likewise, **Spanish** procedural legislation provides only for the general obligation to report facts on a possible crime to the police, prosecutor, or investigating judge.[31] In addition, there is a general provision on cooperation in Article 4 of the law on the National Intelligence Centre (CNI), which refers to the coordination of action between different government bodies. In practice, as shared by the Spanish law enforcement agency representatives during the workshop, information obtained by the CNI can be used only for the purpose of state security and strictly for the aim of criminal investigation; it cannot be shared with anyone except the Guardia Civil. Intelligence services can share data for the purpose of criminal investigation only as names or addresses or other identifiers, but they are not allowed to hand over the content of intercepted communications. Since all the information obtained by the CNI is classified, the police authority has no possibility to use this data in court.

Corresponding general provisions on cooperation between different agencies in **Czech** law are, however, very limited by court practice in the Czech Republic – a country with stricter rules on separation than most and the most restricted possibilities for information sharing among the countries included in this study. The Czech Constitutional Court, in judgement No. I. ÚS 3038/07-1 of 29 February 2008, stated that, since the law of criminal procedure does not provide for the possibility to use intercepted data obtained by any other body than law enforcement (police), the principle of legality prohibits using such information as evidence.[32] However, the intelligence agencies in the Czech Republic are still obliged to provide data to the police pursuant to general provisions in Section 8 Para. 3 of Act No. 153/1994 Sb. on Intelligence Services if findings fall under police jurisdiction. According to the Czech Constitutional Court, this information may not be too specific and contain too many details. A similar general authorisation is outlined in Section 78 of Act No. 273/2008 Sb. on the Police of the Czech Republic, which allows the police to pass information on to security agencies if it is necessary to perform tasks within the scope of their activities. In both cases, however, the provisions are general and do not specifically regulate the sharing of data gained from the interception of communications.[33] At the law enforcement workshop in the Czech Republic, the Czech representatives stated that sharing data between police and security agencies

---

[30] Ibid.

[31] Spanish country report, Chapter I.A.4.a. referring to Articles 259, 262, and 264 LECRIM.

[32] Czech country report, Chapter I.A.4. referring to Para. 25 of the decision of the Czech Constitutional Court No. I. ÚS 3038/07-1 of 29 February 2008.

[33] Ibid.

is almost impossible due to the strict rules and the Constitutional Court's practice. There is an ongoing discussion, however, on the need for specific regulation and on possible legal reform allowing data transfers in certain very limited cases.

The **Polish** report indicates that there is no direct regulation on the transfer of telecommunication data gathered under different regimes from one competent authority to another. However, as there is no prohibition on such sharing of information, various agencies are entitled to obtain personal data and other information gathered by other agencies and services as a result of operational and exploratory activities.[34]

B. Statistics on Telecommunications Interception

Although the national reporters were initially asked to provide statistics on telecommunications interception in the course of this project, a comparison of the statistical data presented in the national reports is not significant for the purpose of the current study due to the different methodologies of collecting and reporting information and the different ways of providing such data. Even at the national level, the analysis of statistics is not always straightforward, and the statistics stem from different sources, e.g. law enforcement agencies and telecommunications providers. For example, the **Swedish** report points out that data on interception warrants and authorisation to obtain metadata might overlap, since one person might be subject to both.[35] Similarly, **Czech** law enforcement agencies confirmed during the workshop that statistics might not always be relevant because (a) they might overlap in some of the cases; or (b) might not fit into the specific calendar year; or (c) a case might involve several warrants and many requests for data from communications intermediaries that might contribute to the significant increase in the statistical number of requests, especially as reported by the service providers.

At the national level, however, the publication of statistical data serves to make law enforcement work transparent and allows for the indication of at least certain trends in the application of interception measures. An obligation to collect and report statistics on communications interception exists in **Australia**, **Austria**, **Belgium**, **France**, **Germany**, **Poland**, **Sweden**, and the **United Kingdom**. National reporters from the **Czech Republic** indicated that, although there is no legally established duty for law enforcement to collect statistics, data is publicly available. In the **Czech Republic**, despite the absence of such an obligation in the law, the police are required under internal regulations to publish analytical and statistical information, including data on the interception of communications.[36] Some of the

---

[34] Polish country report, Chapter III.A.4.

[35] Swedish country report, Chapter I.B.2.

[36] Czech country report, Chapter I.B.1.

country reports, like that from **Belgium**, also refer to statistics in the transparency and disclosure reports from electronic communications service providers, e.g. Google, Vodafone, Microsoft, etc., as to the assessment of the number of requests coming from law enforcement agencies. In some other countries, like in **Spain**, a requirement to compile statistics does not exist, and statistical data are not currently available to the public. All the statistics concerning the interception of communications can be found in the respective country reports.

II. Principles of Telecommunications Interception in Constitutional and Criminal Procedural Law

A. Constitutional Safeguards of Telecommunications

Protection of the privacy of communications is one of the fundamental principles of human rights. On the international level, Article 17 of the United Nations International Covenant on Civil and Political Rights protects privacy and **correspondence** against arbitrary or unlawful interference. On the European level, the safeguards related to private communications can be found in Article 8 of the European Convention on Human Rights and specifically in Article 7 of the Charter of Fundamental Rights of the European Union – "Respect for private and family life," which mentions **communications** as one of the fundamental rights to respect. The fundamental principles and safeguards of privacy and family life are reflected in the national legislation of the countries included in this study. This chapter **analyses** and compares the national approaches to the constitutional safeguards related to the interception of communications.

1. Areas of constitutional protection

a) Secrecy of telecommunication

Among the eighteen countries included in this report, only one – the **United Kingdom** – has no written constitution. In most of the other jurisdictions, the secrecy of telecommunications is a matter of constitutional protection. An analysis of the national legislation shows that such protection can either be provided for in the specific constitutional norms related to the secrecy of communications or fall under the general constitutional protection of privacy. The exception is the Australian Constitution, which by its nature is focused on governance structures of the country and, thus, does not enshrine specific rights, such as a right to privacy.[37]

Most of the countries followed the first approach and adopted a **specific provision in their constitutional law**, which either refers only to telecommunications or

[37] Australian country report, Chapter II.A.1.

protects any correspondence in a more general way. In **Germany**, Subsection 2 of Article 10 of the German Constitution provides protection for the secrecy of telecommunications (which refers both to content and metadata) by requiring statutory authorisation for any infringements.[38] The same approach is taken in **Austria**, where the secrecy of telecommunications is protected by Article 10a of the Basic Law on the Rights of Nationals.[39] Article 49 of the **Polish** Constitution explicitly protects the confidentiality of communications.[40] In **Croatia**, the **Czech Republic**, **Italy**, the **Netherlands**, **Portugal**, and **Spain**, constitutional laws safeguard the secrecy of communications under the provisions of protection of any correspondence including by telephone, telegraph, and other facilities. These provisions stipulate that interceptions can take place only when provided for in the law and with proper court authorisation.[41] In **Belgium**, the privacy of communications is protected by a special provision in the Belgian Constitution, namely Article 29, which stipulates the right to secrecy of communications, and additionally by the constitutional right to privacy in general (Article 22 of the Constitution).[42] Similarly, the **Swedish** Constitution has two relevant provisions: one specifically protecting the privacy of correspondence, including telecommunications, and one on privacy, prohibiting significant privacy invasions without consent.[43] In **Hungary**, the protection of communication falls under the right to privacy stipulated in Article VI of the Fundamental Law of Hungary.[44]

Two of the countries included in this study – **France** and the **United Kingdom** – have no specific constitutional norms related to the secrecy of telecommunications and safeguard it under **general privacy provisions**. **French** constitutional law does not explicitly protect electronic communications and refers only to the respect for private and family life.[45] This general rule considers protection of "the secrecy of electronic communications, personal data, the secrecy of computer data, and confi-

---

38 German country report, Chapter II.A.1.a.

39 Austrian country report, Chapter II.A.1.

40 Polish country report, Chapter II.A.1.

41 Croatian country report, Chapter II.A.1. referring to Articles 35–37 Croatian Constitution; Czech country report, Chapter II.A.1.a. referring to Article 13 Charter of Fundamental Rights and Freedoms; Dutch country report, Chapter II.A.; Italian country report, Chapter II.A.1. referring to Article 15 Constitution; Portuguese country report, Chapter II.B. referring to Article 34 Constitution; Spanish country report, Chapter II.A.

42 Belgian country report, Chapter II.A.1.a.

43 Swedish country report, Chapter II.A. referring to Instrument of Government 2:6 Para. 1, 2.

44 Hungarian country report, Chapter II.A.1.

45 French country report, Chapter II.A.1. referring to Articles 2 and 4 French Human and Citizens Rights Declaration of 1789 and to the French Constitutional Council, Decision n° 2004-492 DC of 2 March 2004.

dential words and images" in accordance with the interpretation of the French Constitutional Council.[46]

The **United Kingdom** has no written constitution and, thus, no constitutional provision on the secrecy of communications. However, the Human Rights Act 1998 requires any public bodies to carry out their activities in accordance with the European Convention on Human Rights. In this regard, Article 8 of the European Convention on Human Rights, concerning the right to privacy, is relevant for the secrecy of communications. However, as noted by the UK country reporter, Article 8 will cease to be an enforceable right under domestic law after the UK's exit from the EU.[47]

b) Confidentiality and integrity of information systems

In addition to the constitutional protection of the secrecy of communications, the **German** report points out the existence of the constitutional protection of confidentiality and the integrity of information systems as a fundamental right.[48] Other national reports provided no information on the existence of any similar provisions – only the **Czech** country report mentions that such constitutional protection might theoretically result from fundamental rights but, in general, the systems are protected by special legislation, e.g. the Cybersecurity Act. Thus, it can be assumed that the case of Germany considering the integrity of information systems worthy of protection within the realm of constitutional law currently remains unique.

The constitutional protection of the fundamental right to confidentiality and integrity of information technology systems in **Germany** was developed by the decision of the German Federal Constitutional Court of 27 February 2008 (1 BvR 595/07), which states that this right originates from the "general right of personality," provided for in Article 2.1 in conjunction with Article 1.1 of the German Constitution. The judgment states that, due to the particular intrusiveness of the "secret infiltration of an information technology system by means of which the use of the system can be monitored and its storage media can be read" it can be allowed only when "factual indications exist of a concrete danger to a predominantly important legal interest."[49] In this regard, according to the Court, the predominant interests can involve "life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence." The judgment pointed out that, in order to justify the intrusion, the facts indicating danger should be assessed in each individual case, even if the threat "cannot yet be ascertained with sufficient probability."[50]

---

46 French country report, Chapter II.A.1.

47 UK country report, Chapter II.A.1.

48 German country report, Chapter II.A.1.b.

49 Ibid.

50 Ibid.

c) Core area of privacy

Another unique area of constitutional protection that exists in **German** law is the concept of the "core area of privacy."[51] This notion includes communications related to the innermost private area of life, such as sexuality or the expression of intimate feelings. Constitutional protection of the core area of privacy requires careful consideration, even before and during the interception of communications, with regard to both avoiding the acquisition of such information and deleting all the data collected if they are related to the core area of privacy.[52] The concept itself and the special protection accorded to this kind of information will be further discussed in the chapter of this study dealing with the prohibition on the interception of privileged communications. While all other country reports indicated that privacy falls under constitutional protection or, as in the case of the United Kingdom, under human rights-related safeguards, no reporter indicated a special concept of the core area of privacy similar to that in German legal doctrine.

d) Right to informational self-determination

Three of the country reports – the **German**, **Italian**, and **Spanish** reports – pointed to yet one more area of protection: the right to informational self-determination. In Spain and Germany, this protection exists on the constitutional level, while in Italy it is stipulated by "soft" law.

The **German** reporters explain this protection as a concept relating to the rights of individuals to take decisions on how they disclose and use their personal data and, in particular, refer to the reasonable faith a person places in the identity of communications partners. Moreover, this principle of guaranteeing informational self-determination safeguards persons against the deliberate collection and analysis of data gathered from publicly available content without a proportional statutory basis. Any infringement of informational self-determination, therefore, has to be justified by a prevailing public interest. In this regard, the special factor for consideration is data relevant to personality. Any intrusion during the investigation is deemed to be of significant invasiveness if the data can lead to conclusions about the "the nature and intensity of interpersonal relationships, personal interests, habits and tendencies, or the content of communication."[53]

A similar concept exists in **Spain**, where the decision of the Constitutional Court 292/2000 made a distinction between the notion of privacy and personal data protection, referring to the "fundamental right to data protection" as the right aiming "to guarantee that the individual has the power of control over their personal data,

---

[51] German country report, Chapter II.A.1.c.

[52] Ibid.

[53] German country report, Chapter II.A.1.d.

its use and destination, in order to prevent any illicit and damaging transfer of those data, that may affect the dignity and the rights of the affected person."[54] According to the national reporter, this decision allows the conclusion to be drawn that the court recognised the right to informational self-determination as a power and right to "control over the information regarding him/herself, about its use and destination, to avoid an illicit use of it."[55]

In **Italy**, informational self-determination is provided for in the "Declaration of Internet Rights" *(Dichiarazione dei diritti in Internet)*, adopted on 28 July 2015 by the "Commission for rights and duties in Internet" of one of the Houses of the Parliament *(Commissione per i diritti e i doveri in internet della Camera dei Deputati)*. Article 6 of the Declaration is dedicated entirely to informational self-determination.[56]

2. Proportionality of access to data

The principle of proportionality is referred to in almost all of the national reports as one of the most important requirements for the interception of communications and any other form of access to data in criminal investigations. The application of the principle of proportionality as one of the substantial prerequisites for any intrusion into the secrecy of communications will be further analysed in this study, especially with regard to the interception of the content of electronic communications.

3. Consequences for the interception of telecommunication

Different safeguards, e.g. constitutional guarantees for the secrecy of communications, privacy, and informational self-determination, together with the application of the principle of proportionality as one of the substantive requirements for any intrusion into a person's private life, have had a number of consequences for the interception of electronic communications. Except for the **United Kingdom**, where the warrant must be approved by a judicial commissioner, legislation in all other jurisdictions requires interception for the purpose of criminal investigations to be authorised by a court (as further analysis will show), with some exception provided for urgent circumstances.

Furthermore, national legislation implements various checks and balances, such as limiting the application of the interception to only certain types of crime, limiting the period of validity of the interception order and the possible number of prolongations, establishing reporting obligations as well as duties and obligations

---

[54] Spanish country report, Chapter II.A.2.

[55] Ibid.

[56] Italian country report, Chapter II.A.1.d.

concerning the destruction of irrelevant information, and many other formal requirements and safeguards. Moreover, since certain types of communication are especially protected at the national level, such as information related to the core area of privacy in Germany or communications related to the attorney-client privilege in some of the countries, the frameworks regulating interception in most of the jurisdictions specifically address this issue by including special rules on protecting this type of communication from interception or by ensuring that such information will not be used in criminal investigations. These issues will be further considered in detail in the following chapters of this study.

4. Statutory protection of personal data

To protect the secrecy of communications, the criminal law in all the countries included in this study has established criminal liability for the unlawful interception of communications. Further regimes of protection at the national level involve the prohibition of access to computer systems and of the interception of computer data, outlined either in the criminal law or in specific cybercrime legislation and other provisions aiming to protect the secrecy of communications and the integrity of data.

As already noted above, another regime of protection includes safeguarding certain information related to professional communications, e.g. those of lawyers, clergymen, medical professionals, journalists, or parliamentarians against the interception of communications, either by imposing a direct prohibition on such interception or by providing for an obligation to delete or not use this information if captured. Additional safeguards in this regard can include the notification of respective professional associations or the technical obligation to filter certain communications. Such obligations and the methods of dealing with privileged information are analysed further in this study.

Four country reports – the **Belgian**, **Czech**, **German**, and **Spanish** reports – also highlight the application of the principle of purpose limitation of personal data, which stipulates that data may be used only for the purpose they were collected for. In accordance with this principle, interception data collected during criminal investigations have to be deleted if they are irrelevant for the investigation or no longer required for the purpose of the criminal prosecution of offences. Other dimensions of this principle can include frameworks limiting the use of collected data in other criminal investigations or rules on the admissibility of evidence resulting from the interception of communications.

B. Powers in the Code of Criminal Procedure

Most of the country reports state that the requirement for reasonable clarity of powers in the law of criminal procedure, related to the principle of legality, is one

of the basic conditions in their respective legislation. However, although national reporters refer to the prohibition on using the powers by analogy as the underlying basis of this principle, some of the country reports, such as the **Swedish** report, question this principle and point out that, in fact, some of the technology-neutral language in the national laws of criminal procedure allow the new techniques to be used to acquire data under existing legal provisions.[57]

The powers provided in the law of criminal procedure related to interception of the content of communications, remote data capture, interception of and access to traffic data, and access to subscriber data in the jurisdictions included in this research study are outlined and analysed in the following chapters.

III. Powers for Accessing Telecommunication Data in the Law of Criminal Procedure

A. Overview

This chapter aims to provide a comprehensive comparative analysis of powers for accessing telecommunication data under the law of criminal procedure of the countries included in this study. In addition to a detailed evaluation of all the aspects concerning the power of law enforcement agencies to acquire communications in the course of their transmission, this analysis includes a comparison of the national laws related to such investigative measures as collection of traffic data and subscriber data, search and seizure of electronic data, and additional instruments like the use of IMSI catchers.

B. Interception of Content Data

1. Statutory provisions

The following provisions of the national legislation have been indicated in the country reports as the main legal basis for the power of law enforcement agencies to intercept communications for the purpose of criminal investigations:

- **Australia**: Chapter 2 of the Telecommunications (Interception and Access) Act 1979 (TIA Act)
- **Austria**: Section 134 (3) StPO
- **Belgium**: Article 90*ter* Code of Criminal Procedure
- **Croatia**: Chapter XVIII, sections 12 and 13 Criminal Procedure Act

---

[57] Swedish country report, Chapter II.C.

- **Czech Republic**: Section 88 Code of Criminal Procedure
- **Estonia**: Section 126[1] Code of Criminal Procedure
- **France**: Article 100 Penal Procedure Code
- **Germany**: Section 100a Subsection 1 StPO
- **Hungary**: Sections 231–236 Criminal Procedure Act
- **Italy**: Articles 266–270 Code of Criminal Procedure
- **Netherlands**: Article 126m Code of Criminal Procedure
- **Poland**: Chapter 26 Code of Criminal Procedure (Articles 237–242)
- **Portugal**: Articles 187–190 Code of Penal Procedure
- **Spain**: Article 588 LECRIM
- **Sweden**: Section 27:20 SJP
- **Switzerland**: Article 269 Swiss Code of Criminal Procedure
- **United Kingdom**: IPA 2016
- **United States**: ECPA (Electronic Communications Privacy Act), FISA (Foreign Intelligence Surveillance Act)

2. Scope of application

a) Definition of "communication"

Prior to the development of information and communication technologies and the use of digital networks, the interception of voice traffic in circuit-switched telecommunications systems was direct and unsophisticated – compared to today's situation. With the availability of changing communications patterns and the use of different communications channels, however, the scope of the interception of both traffic data and content data has widened. Growing numbers of devices are moving increasing amounts of data across networks by means of different technologies and services. Moreover, with the development of machine-to-machine communications, meaning that technology allows wireless and wired systems to interact with other devices without the involvement of a direct human component, it is very important to understand whether the scope of national legislation covers all types of communication in the interconnected world and whether the law of criminal procedure can address the emerging technical complexity.

National criminal procedure can define the object of interception in different ways, usually by using such generic terms as "telephone communication," "electronic communications," or "electronic communications between persons." The legislation in the eighteen jurisdictions included in this study varies from country to country concerning the use of these generic terms with regard to the object of interception.

The first group of countries uses the term "**telecommunications**." In **Germany**, the object of interception is defined as "telecommunication" and in the **Czech Republic** as "telecommunications traffic." The second most common reference is the use of the term "communication" in different variations: For example, the legislation of the **United Kingdom** defines the object of interception as "communication" and **Swedish** and **Belgian** laws use the term "electronic communication."[58] Procedural law in the **Netherlands** describes the object of interception by using an additional clause referring to the privacy of communications, namely ".non-public communication."[59] The **Spanish** law of criminal procedure refers to the interception of "telephone and electronic communications." **Austrian** criminal procedure law defines interception as "surveillance of messages" that are sent, transmitted, or received by a natural person via a "communications network."[60] Similarly, **French** legislation defines the object of interception as "correspondences transmitted by means of electronic communications."[61]

Some of the national laws refer to telephone communications. For example, the **Polish** Code of Criminal Procedure defines the object of interception as "content of telephone conversations" and further extends the application of the respective provisions to content transmitted using forms of information transfer other than telephone.[62] **Croatian** law of criminal procedure refers to both "telephone conversations" and "other means of remote technical communication."[63] **Italian** legislation defines the object of interception as "conversations," "telephonic communications" and "other forms of telecommunications."[64]

Some of the national reports refer to the lack or even absence of a definition concerning the generic terms "communications" or "telecommunications" in the law of criminal procedure for the purpose of interception in their respective jurisdictions. As the analysis shows, when a definition exists, it can be found either in the special legislation on telecommunication, as in **Germany** and **Sweden**, or in the law of criminal procedure, as in the **United Kingdom**. The **Czech** and **French** national reporters specifically pointed out the lack of a statutory definition of communications for the purpose of interception and referred to the relevant discussions on this issue in the academic literature.

---

58 Belgian country report, Chapter III.B.2.; Swedish country report, Chapter III.B.1.

59 Dutch country report, Chapter III.B.2.a.

60 Austrian country report, Chapter III.B.1.

61 French country report, Chapter III.B.2.a.

62 Polish country report, Chapter III.B.2.

63 Croatian country report, Chapter III.B.1

64 Italian country report, Chapter III.B.2.

– *Statutory clarification in special legislation on telecommunications*

Two countries – **Germany** and **Sweden** – reported that, despite the lack of a comprehensive definition in the procedural law, the related terms can be found in the **special legislation on telecommunications or electronic communications**, thus providing the possibility for judicial interpretation. However, even such reference might not be able to solve all the problems related to the possible scope of the object of interception. As highlighted in the **German** national report, the understanding of the term "telecommunications" is established through the interpretation of the special telecommunications regulation in combination with judicial practice. In judicial practice, the meaning of "telecommunication" is understood as "incorporeal transmission of information through electromagnetic or optical signals, similar to the interpretation in the Telecommunication Act."[65] This interpretation, however, does not address all the concerns related to the scope of the interception object. On the contrary, according to the German country report, the lack of an exact meaning and the absence of a proper statutory clarification raise numerous issues related to the application of the interception provision.[66]

A similar definition of the object of interception can be found in **Swedish** law on electronic communications, although no discussion similar to the German debate was mentioned in the Swedish country report. As pointed out in the Swedish national report, the Electronic Communications Act 2003 provides an explanation of the term "communication." Article 6:1 of the Act defines it as follows:

> any information exchanged or transmitted between a limited number of parties through a publicly available electronic communications service, except information which is transmitted as part of the broadcasting of radio and television programs that are targeted to the general public…[67]

The national report further notes that this definition, together with Article 1:7 of the same law, which defines "electronic communications network," gives a clear interpretation of the term "communications" for the purpose of defining the scope of the procedural provisions related to interception.

– *Statutory clarification in procedural law*

The laws in the **United Kingdom** and **Australia** directly explain the meaning of the term "communication" within their procedural framework on interception of communications. The IPA in the UK and the Australian TIA Act provide for precise definitions of communication, thus defining the scope of interception.[68]

---

65 Cited from German country report, Chapter III.B.2.a.

66 German country report, Chapter III.B.2.a.

67 Swedish country report, Chapter III.B.1.

68 Australian country report, Chapter III.B.2.; UK country report, Chapter III.B.2.

– *No precise statutory definition*

National reporters from the **Czech Republic** and **France** referred to the lack of legal clarity concerning the definition of the object of interception and provided an overview of the discussions in the academic literature.

In the **Czech Republic**, according to the national reporter, the special legislation on telecommunications, namely the Act on Electronic Communications,[69] does not provide a statutory clarification of the term "telecommunications traffic" used in procedural law. However, the debates in the academic literature, together with an analysis of the special legislation, enable the conclusion that the object of interception can be interpreted as "content transferred via electronic communications networks, which are defined in the electronic communications legislation as transmission systems and, where applicable, switching or routing equipment and other facilities, including network elements which are inactive and which permit the conveyance of signals."[70]

Like in the Czech Republic, legislation on electronic communications and criminal procedure in **France** uses different terms for what can be described as "communication" for the purpose of interception, thus creating a lack of clarity concerning a comprehensive legal definition of the object of interception. In this regard, the French country report refers to the necessity of interpreting the scope of the application of the interception provision by means of analysis of the academic literature together with civil legislation, the French Code on Penal Procedure, and special legislation on electronic communications. The academic literature in France perceives the object of interception of communications – "correspondence" – as personal and actual communication, which allows interactivity, and which is addressed to specific and individualised persons.[71] Furthermore, according to the report, the term "electronic communications" is defined in the special legislation as "emissions, transmissions or reception of signs, signals, writings, images or sounds, by electro-magnetic means."[72]

b) Content of communications: communication between persons

The growing technical complexity of networks and services, on the one hand, and the lack of a precise statutory definition of communications for the purpose of interception in criminal procedure in many countries, on the other, raise a very

---

[69] Czech country report, Chapter III.B.2.a.

[70] Czech country report, Chapter III.B.2.a. referring to Section 2 of Act No. 127/2005 Sb., on electronic communications.

[71] French country report, Chapter III.B.2.a.

[72] French country report, Chapter III.B.2.a. quoting Article L.32-1 Post and Electronic Communications Code (PECC).

important question as to what extent the new types of electronic communication and services are covered by procedural law. While some of the national reporters state that the legislation in their respective jurisdictions is technology-neutral enough to cover the interception of other communication, such as IP traffic between independent computer systems, others highlight the problems and ongoing debates related to machine-to-machine communications. The ability of the traditional interception legislation to cover all types of modern communications is not always straightforward. The lack of a clear legal definition in some of the jurisdictions raises certain questions related to new types of information transfer and to the differences between interception of person-to-person and machine-to-machine communications. While the legislation in such jurisdictions as the **United Kingdom** or **Australia**, where the term "communications" is defined precisely in procedural law, covers every type of traffic, other countries, like **Germany** and **Belgium**, are currently debating the difference between person-to-person and machine-to-machine communications. These discussions are generally related to the notion of the "human" component of communications for the purpose of interception as opposed to the "machine-to-machine" interactions. **Austrian** reporters highlighted the same issue: The definition of communication for the purpose of interception only includes types of communications that involve at least one natural person, therefore the surveillance of autonomous communications, e.g. between two machines (M2M communication) is not covered.[73]

The **German** country report points out that, for the purpose of interception, legislation in Germany refers to a person exchanging information via telecommunications equipment; this conflates a wide range of possible ways to transfer information, from the automated arrival of data in voicemail and e-mail boxes to failed attempts to establish a communication connection. The reference to a personal, human component in current court practice, however, means that communication transmissions carried out only between technical devices are covered by the scope of the interception provision only when such data exchanges take place to establish a connection or transfer information with the final aim of facilitating communications between human beings. Consequently, the data transfers occurring between mobile devices in standby mode, for example to convey signals of readiness to operate, do not constitute telecommunication according to a decision of the German constitutional court. So far, however, it has been clarified neither on the academic level nor in court practice to what extent this interpretation can be applied to IP traffic.[74]

Other difficulties related to the possible coverage of different types of communications are highlighted in the Belgian national report. As was already mentioned in the previous section of this study, in **Belgium**, the question of what constitutes the

---

[73] Austrian country report, Chapter III.B.2. referring to ErlRV 17 BlgNR XXVI. GP, 8.

[74] Geman country report, Chapter III.B.2.a.

content of communications for the purpose of interception in criminal investigations, in addition to analogous communications between persons, is a matter of debate in the academic literature. The Belgian reporter states that it is commonly agreed in the literature that, in addition to the conventional analogous communications, Belgian procedural law covers different types of data transfer between persons, e.g. various services related to e-mail, instant messaging via different applications and services (including mobile applications), Voice-over-IP traffic, etc.[75] However, according to the report, "IP data does not constitute private communications and therefore does not fall under the scope" of the interception provision.[76] The national reporter also refers to the non-inclusion of cases of interception of cloud computing communications and machine-to-machine communications in the annual reports published by the Minister of Justice.[77]

France represents a distinct case due to the existence of several interception-related investigative measures in its legislation on criminal procedure. According to the French national report, the analysis of the scope of the provision on the interception of correspondence, together with special legislation on electronic communications, leads to the conclusion that the object of interception covers all technologies that enable the emission, transmission or reception of correspondence by electromagnetic means, according to the legal definition of electronic communication, *inter alia* intercepted analogous communication (voice and data) via landlines and IP traffic of a person-to-person communication, including through a mobile broadband modem.[78] Thus, French legislation also seems to have the notion of a "human" component in relation to the interception of communications. Furthermore, according to the French country report, interception of other types of information transfer, such as data traffic between human beings and automated systems, including communications with a cloud and also machine-to-machine communications, would instead fall under the scope of provisions of criminal procedure other than the interception of private correspondence. The report lists search and seizure and norms regulating interception with the use of remote forensic software among these procedures.[79]

By contrast, some of the national reports, such as the **Italian** report, point out that the definition of communications for the purpose of interception is sufficiently broad to cover all types of communications and traffic. In Italy, Article 266*bis* Code of Criminal Procedure allows interceptions of the "flow of communications

---

[75] Belgian country report, Chapter III.B.2.a. referring to *Kerkhofs*/*Van Linthout*, Cybercrime, Politeia, 2013, pp. 279, 282, 295.

[76] Belgian country report, Chapter III.B.2.a.

[77] Ibid.

[78] French country report, Chapter III.B.2.a.aa.(2).

[79] Ibid.

related to cyber- and telematic systems, or between different systems;" this wording is broad enough to include machine-to-machine communications.[80]

c) Current matters of dispute

Most of the countries included in this study indicated further challenges related to the definition and scope of the interception of communications provisions in the modern digital era. These challenges involve the temporary limits of communications and the blurring lines between communications in transmission and stored communications, as well as issues related to the use of remote forensic software for capturing data and to the possibility of accessing the communication system remotely to install such software. Further matters of dispute include the use of passwords to access e-mail boxes and the interception of communications between computer and storage media. These challenges will be discussed in the respective chapters of this report.

3. Special protection of confidential communication content

a) Privileged communication

The protection of certain types of privileged communication from interception represents one of the most significant divergences in the law and practice of the countries included in this comparative study. Professional confidentiality and the privacy of persons are protected in national laws by systems of different safeguards that regulate which information cannot be captured during the course of interception and regulate how to deal with information obtained in practice if an acquisition takes place. The current state of legal approaches to safeguarding professional secrecy and certain types of other privileged communication against interception can be characterised as a patchwork of various legal rules. These rules range from detailed and extensive protection regimes, such as those existing in **Germany** and **France**, to the prohibition on interception of only one particular type of professional secrecy, such as lawyer-client communications in the **Czech Republic**.

The divergences in the national laws can be attributed to a number of different matters. First of all, the prohibition on the interception of a certain type of communication is not always straightforward: there are different types of protection. Protection can be conditional or unconditional, or the rules of protection against interception can distinguish between prohibition on recording and prohibition on transcription of certain privileged communications. Secondly, differences exist in the nature of the content that is safeguarded against interception: while the rules on protection of certain types of communication include professional privileges in all

---

[80] Italian country report, Chapter III.B.2.

of the countries, in **Germany** there is an additional area of protection that refers to the private nature of communications beyond professional privileges – the core area of privacy. Thirdly, the types of professional communications protected against interception may vary significantly from one country to the next with regard to which professions enjoy special privileges. All these variables contribute to the complexity of the system of protection of privileged communications and can thus become a very complicated issue for cross-border cooperation involving the interception of safeguarded content, especially with regard to the possibility of direct data transfers in the context of mutual legal assistance.

Taking into account the complexity of the national approaches to the interception of privileged communications and the different variables concerning the type and nature of protection, this chapter approaches the comparison of national legislation as follows: Firstly, it analyses various **types of protection**, such as **conditional and unconditional protection**. This comparison is taken further in the second part of the analysis, namely the protection of communication content specifically related to **different types of protected communication**, such as professional communication and the core area of privacy. The combination of both factors – types of protection and types of protected communication – in a comparative analysis allows the complexity of the legal regimes of privileged communications to be illustrated. Thirdly, the chapter compares the national legal and practical approaches to dealing with privileged communications in the course of interception, e.g. blocking, deletion, and prohibition on use in court proceedings.

aa) Types of protection

An analysis of the national laws shows that the protection of certain types of communication from interception is not uncomplicated and cannot always be prescribed. From the national law comparison of the countries included in this study, two diverging factors can be found. The first one is conditional and unconditional protection, which can be found in **Germany**, and the second is the difference between the prohibition on recording of particular communication and protection against transcription when communication is intercepted. The latter regime exists in **Belgium** and **France**. It shall be noted that, as the analysis will elaborate further, both regimes provide no protection in the case of suspicion.

– *Conditional/unconditional protection*

The distinction between conditional and unconditional protection of privileged communications can be found in **German** legislation. These two types of safeguards differ in terms of the object of protection and the consequences of the interception of communications. *Unconditional* protection implies that certain professions are strictly safeguarded from the interception of communications. Any data acquired

despite this strict prohibition cannot be used for the purpose of investigation, not even as a mere clue.[81] If records of such communications are made, they have to be destroyed without delay, but the circumstances of the capture of unconditionally protected communications as well as their deletion must be documented. Provisions regulating unconditional privilege also cover cases in which any information related to unconditionally protected communications is obtained accidentally during the interception. This type of privilege is provided for in Section 160a Subsection 1 (1) in connection with Section 53 StPO for certain types of professional communication, e.g. clergymen or attorneys.[82]

The second type of protection – *conditional* protection – refers in Germany to the safeguarding of certain professions from the interception of communications, depending on the gravity of the offence for which interception is used in the criminal investigation. The prohibition on interception here depends on the principle of proportionality and on balancing the interests of the investigation with the protection of professional secrecy of certain types of communication. Conditional protection against interception is provided for by Section 160a Subsection 2 and Section 53 StPO. As far as the interception of conditionally protected communication is concerned, Section 160a Subsection 2 StPO stipulates that the question of whether the measure is applicable or not depends on the proportionality of the intrusion. The key criterion for reviewing proportionality is the significance of the criminal offence being investigated.[83] As stated in the German country report, unless the criminal investigation is carried out in relation to an offence of substantial significance, legal protection from interception is very likely to be granted to the conditionally protected communication or, at least, the execution of the interception might be limited. The principle of proportionality also applies to the analysis of the results of the interception related to conditionally protected professional secrets. When criminal offences are considered to be of substantial significance in an investigation, the possibility of using interception as an investigative measure depends on balancing the interests of the criminal investigation, on the one hand, and, on the other, the legally protected public interest as well as the interests of the person who entrusted certain information to the professional falling under the privileged category.[84]

---

[81] German country report, Chapter III.B.3.a.

[82] For a detailed list of professions, see German country report, Chapter III.B.3.a.

[83] According to the German country report (Chapter III.B.3.a.), "a criminal offence of substantial significance can be assumed when the specific offence exhibits at least an intermediate level of criminality, significantly disturbs peace under the law, and is suited to significantly compromise the population's sense of legal security. These prerequisites are usually not met when the offence is punishable by a maximum prison sentence of less than 5 years."

[84] German country report, Chapter III.B.3.a.

– *Prohibition on recording and prohibition on transcription*

This distinction can be found in the interception legislation of **France** and **Belgium**, which differentiate between prohibition on interception concerning certain professions enjoying privileged regimes and prohibition on the transcription of certain types of communication related to specially protected professional secrets. In **France**, the law of criminal procedure provides a complex set of measures protecting privileged communications against interception: Article 100-7 Penal Procedure Code provides for strict safeguards in relation to several types of professional communications, thus prohibiting their capture. However, in addition to this prohibition, Article 100-5 Penal Procedure Code stipulates protection against transcription for certain types of professional communication.[85]

Similar provisions can be found in the **Belgian** law of criminal procedure, which distinguishes between interception and the official transcription (records) of communications of certain professions unless special conditions are met. The first type of protection against interception is provided for by Article 90*octies* Para. 1 and 2, 1° CCP, which establishes a special regime of privileged communications with a strict prohibition on interception. In addition to this safeguard, Article 90*sexies* Para. 3, 1° CCP prohibits the inclusion of several types of professional communications in official transcripts. This prohibition covers a broader range of confidentiality related to professional activity than the legal provision on protection against interception. The Belgian report notes that, although recordings protected by the rules on privileged communications cannot be included in official records, they must be retained in a sealed envelope,[86] because interested parties (e.g. defendant, accused, and others) can lawfully demand access to the investigation material.[87]

– *Legal regimes of protection with no distinctions between the types of protection*

Other countries have more general and less complex legal regimes of protection of professional secrecy. In **Croatia**, **Estonia**, **Hungary**, **Italy**, the **Netherlands**, **Poland**, **Portugal**, **Spain**, **Sweden**, and **Switzerland**, this protection refers to the exemption from the duty to testify in court or to the right of non-disclosure. For example, in **Sweden**, Article 27:22 CJP prohibits the interception of communications of persons who cannot be called as a witness in criminal proceedings due to their professional activity.[88] In **Croatia**, Article 285 Criminal Procedure Act contains a list of exemptions from the duty to testify and covers a number of profes-

---

[85] For a detailed list of professions, see the French country report, Chapter III.B.3.

[86] Belgian report, Chapter III.B.3.a. referring to Article 90*septies* Para. 3 CCP.

[87] Belgian country report, Chapter III.B.3.a. referring to Article 90*septies* Para. 5–7 CCP.

[88] The list of such professions is provided for in Article 36:5 CJP. See Swedish country report, Chapter III.B.2.

sions that enjoy privileged communications.[89] Similarly, in the **Netherlands**, a general provision covering professional secrecy – Article 126aa in conjunction with Article 218 Code of Criminal Procedure – prohibits the interception of information related to professional secrets for persons with a right to non-disclosure.[90] In **Spain**, the provisions on the interception of communications explicitly protect only one category: privileged communication between the suspect and his/her defence lawyer. However, Spanish law on criminal procedure – Article 417 LECRIM and Article 20.1 of the Spanish Constitution – establishes a general protection regime of professional secrecy by exempting journalists from the duty to testify, which is considered a constitutional protection of journalists' professional secrets, namely their sources of information.[91]

The least complex set of measures protecting professional secrecy exist in the **Czech Republic** and **Australia**. According to the Czech national report, only communication between the defence council and the accused falls under the privilege and could be the subject of the prohibition on interception.[92] In **Australia**, the definitive law on professional legal privilege can be found in a decision of the High Court. While the decision does not prohibit the interception of such communication, it states that "the privilege survives so as to render the intercepted communications inadmissible in subsequent proceedings."[93]

bb) Protected communications

Most of the countries have legislation providing for the protection of professional secrets against telecommunications interception; however, the types of professions protected and the conditions for protection can vary significantly. There are various approaches to which communications are to be protected, to the protection of either professional secrecy or privacy or both, and to different practical consequences of such prohibitions for criminal investigations. In general, two types of protected communication can be found in national legislation. The first type of protection refers to different **professions** protected by virtue of law as privileged communications. The second type refers to communications protected on account of their special nature – this type of protection can be found in Germany and concerns information related to the "**core area of privacy**." The following analysis compares the details and divergences of such protection for both types.

---

89 Croatian country report, Chapter III.B.3.

90 Dutch country report, Chapter III.B.3.

91 Spanish country report, Chapter III.B.3.a. and Chapter II.A.4.b.

92 Czech country report, Chapter III.B.3.a.

93 Australian country report, Chapter III.B.3.

– *Privileged professions*

Some of the complex protection regimes, like those in **Austrian**, **Belgian, French**, or **German** law, provide more sophisticated protection with reference to conditional and unconditional protection or the distinction between recording and transcribing privileged communications. The most commonly protected professions are lawyers (in particular defence attorneys), medical professionals, clergymen, journalists, public notaries, and members of parliament. However, even when legislation in different countries refers to the same professional activity, the scope of protection might still differ. These divergences are based on the different types of protection that were explained in the previous part of this chapter, such as conditional and unconditional protection, or the distinction between recording and transcripts. Further analysis will provide insight into these divergences on the national level, with regard to the most common protected professional privileges. It shall be noted here that protection against interception deriving from a professional privilege is not absolute: exemption from such protection in a case of suspicion is further analysed in this chapter.

Lawyers, **in particular defence attorneys**, are protected in most of the countries, based on the notion of a privileged communication between lawyer and client. In the more complex regimes of privileged communication, this profession enjoys the highest level of safeguards against interception. **German** law (Section 160a Subsection 1 (1) in connection with Section 53 StPO) protects defence counsels of the accused and attorneys unconditionally. Furthermore, in Germany, the unconditional protection provisions also extend to assistants to defence lawyers and attorneys as well as trainees involved in the professional activity.[94] The **French** and **Belgian** codes of criminal procedure[95] exempt this type of communication from both recording and transcription. The **Czech** and **Spanish** laws of criminal procedure explicitly protect communications between the defence council and the accused in the provisions related to communications interception.[96] The **Netherlands** provide such protection under the right of non-disclosure for lawyers.[97] **Austrian**, **Croatian**, **Estonian**, **Italian**, **Polish**, **Portuguese**, **Swedish**, and **Swiss** laws exempt communication between lawyer and client under the prohibition on interception of communications for persons who cannot be called as a witness in criminal proceedings due to their professional activity and, therefore, their professional

---

[94] German country report, Chapter III.B.3.a.

[95] French country report, Chapter III.B.3. referring to Articles 100-7 and 100-5 Code of Criminal Procedure; Belgian report, Chapter III.B.3.a. referring to Article 90*octies* Para. 1 and 2, 1°, Article 90*sexies* Para. 3, 1° CCP.

[96] Czech country report, Chapter III.B.3. referring to Section 88 Para. 1 Code of Criminal Procedure; Spanish country report, Chapter III.B.3.a. referring to Article 118.4 LECRIM.

[97] Dutch country report, Chapter III.B.3.

communications with the clients are protected against interception.[98] In **Hungary**, the lawyer-client privilege is provided for in special legislation concerning the activities of attorneys.[99] In **Australia**, relevant protection exists in court practice: while interception is possible, the lawyer-client privilege exists to render intercepted communication inadmissible as evidence.[100] According to the country reports, lawyer-client privilege also exists in the **United Kingdom** and the **United States**.[101]

Several countries included in this study provide special protection for communication of **clergymen**. This type of communications is the subject of unconditional protection under the **German** law.[102] **Austria** has a special provision in criminal procedure law specifically protecting communication of clergymen.[103] **Estonian**, **Hungarian**, **Italian**, **Polish**, **Swedish**, **Spanish**, and **Swiss**[104] legislation provides special safeguards against the interception of clergymen's communications under the rules covering exemptions from the duty to testify, and **Dutch**[105] law does so under the right of non-disclosure.

The communication of **medical professionals** is another type of professional secrecy that has been given special protection in many of the national laws: many countries provide special safeguards for this type of communication. In **Germany**, however, compared to the unconditional protection of defence lawyers and clergymen, the communication of doctors is protected only conditionally and is thus subject to assessment in accordance with the principle of proportionality, and it must be balanced with the interests of the investigation.[106] By contrast, in **Belgium**, med-

---

98 Austrian country report, Chapter III.B.1.3.; Croatian country report, Chapter III.B.3., referring to Article 285 CPA; Estonian country report, Chapter III.C.; Italian country report, Chapter III.B.3.; Polish country report, Chapter III.B.3.; Portuguese country report, Chapter III.B. and information from the law enforcement workshop in Portugal; Swedish country report, Chapter III.B.2. referring to Article 27:22 CJP; Article 171 Swiss Code of Criminal Procedure.

99 Hungarian country report, Chapter III.B.3.

100 Australian country report, Chapter III.B.3.

101 UK country report, Chapter III.B.3.a.; USA country report.

102 German country report, Chapter III.B.3.a. referring to Section 160a Subsection 1 Section 1 in connection with Section 53 StPO.

103 Austrian country report, Chapter III.B.3.

104 Estonian country report, Chapter III.C.6. referring to § 72 Code of Criminal Procedure; Italian country report, Chapter III.B.3.; Polish country report, Chapter III.B.3.; Swedish country report, Chapter III.B.2. referring to Article 27:22 CJP; Spanish country report, Chapter III.B.3.a. referring to Article 417 LECRIM; Article 171 Swiss Code of Criminal Procedure. Hungary and Switzerland: information obtained during the law enforcement workshop.

105 Dutch country report, Chapter III.B.3.

106 German country report, Chapter III.B.3.a. referring to Section 160a Subsection 2 and Section 53 StPO.

ics' communications are protected from both recording and transcription.[107] In **France**, a doctor's premises are explicitly protected against the use of remote forensic software, while the interception of communications without the use of remote forensic software can still be performed.[108] **Croatia**, **Estonia**, **Hungary**, **Italy**, the **Netherlands**, **Poland**, **Sweden**, and **Switzerland** protect doctors under provisions providing protection for other professional secrets.[109]

Journalists are also the subject of conditional protection in **Germany**[110] and exempted from transcription of interception in **Belgium**.[111] **French** law approaches the protection of journalists differently, depending on whether the use of remote forensic software or the interception of communications is concerned. The law provides a strict ban on the use of remote forensic software on business premises and in company vehicles of media companies, audio-visual communication companies, online public communication companies, and press agencies.[112] With regard to the interception of communication, the French Penal Procedure Code does not prohibit interception but instead establishes additional safeguards against transcription of any correspondence with a journalist, which could enable the identification of "a source in breach of Article 2 of the Law of 29 July 1881 on freedom of the press."[113] In **Spain**, the communications of journalists are protected against interception under the general exemption from the duty to testify in court regarding sources.[114] **Austrian** law protects media owners (publishers), media staff, and employees of a media company or media service with regard to questions that relate to the individual who authored, submitted, or was the informant for the programmes/articles and records, or that relate to communications they receive in view of their occupation.[115] In **Switzerland**, Article 172 Code of Criminal Procedure protects journalists' sources: persons involved professionally in the publication of information in the editorial section of a medium that appears periodically, together

---

[107] Belgian country report, Chapter III.B.3.a. referring to Article 90*octies* Para. 1 and 2, 1°, Article 90*sexies* Para. 3, 1° CCP.

[108] French country report, Chapter III.B.3.

[109] Croatian country report, Chapter III.B.3. referring to Article 285 CPA; Estonian country report referring to Chapter III.C.6., § 72 Code of Criminal Procedure; Italian country report, Chapter III.B.3.; Dutch country report, Chapter III.B.3.; Polish country report, Chapter III.B.3.; Swedish country report, referring to Article 27:22 CJP. Hungary and Switzerland: information obtained during the law enforcement workshop.

[110] German country report, Chapter III.B.3.a. referring to Section 160a Subsection 2 and Section 53 StPO.

[111] Belgian country report, Chapter III.B.3.a. referring to Article 90*sexies* Para. 3, 1° CCP.

[112] French country report, Chapter III.B.3.

[113] Ibid.

[114] Spanish country report, Chapter III.B.3.a. and Chapter II.A.4.b. referring to Article 417 LECRIM and Article 20.1 Spanish Constitution.

[115] Austrian country report, Chapter III.B.3. referring to Section 157 Subsection 1 (3) Austrian StPO.

with their auxiliary personnel. Similar protection of journalist sources exists in **Croatia**, **Estonia**, and **Poland**.[116] In the **United Kingdom**, IPA introduced special provisions related to interception of confidential journalist material in 2016: the existence of arrangements specific to handling, retention, use, and destruction of such material must be taken into consideration by the authority issuing a warrant.[117]

The communication of **public notaries** is yet another type of privilege protected by virtue of law in several countries. **German** and **Swiss** legislation provides conditional protection for this type of professional privilege,[118] **France** protects the premises of notaries against the use of remote forensic software,[119] and **Croatia**, **Estonia**, **Poland**, and the **Netherlands** provide protection of this type of communication under the right of non-disclosure.[120]

Members of parliament are protected against interception in **France**, **Germany**, and the **United Kingdom**. The **German** law of criminal procedure provides unconditional protection for communications of the members of the federal parliament, state parliament, or the European Parliament.[121] **French** legislation prohibits both the interception of electronic communications by parliamentarians and the use of remote forensic software on their office premises, in their vehicles, and in their homes.[122] In the **United Kingdom**, the IPA introduced protection of such communications in 2016.[123]

In addition to the most common protection of professional privileges listed above, national legislation can cover **other types of professional secrecy**. In **Germany**, the Code of Criminal Procedure provides conditional protection against interception for information entrusted to or having become known to individuals acting in their capacity as patent attorneys, certified public accountants, sworn auditors, tax consultants, psychologists, psychotherapists, pharmacists, midwives, members of a pregnancy counselling agency, or drug dependency counsellors in a

---

116 Croatian country report, Chapter III.B.3. referring to Article 285 CPA; Estonian country report, § 72 Code of Criminal Procedure; Polish country report, Chapter III.B.3.

117 UK country report, Chapter III.B.3. referring to Sections s28(3) and 29(3) IPA 2016.

118 German country report, Chapter III.B.3.a. referring to Section 160a Subsection 2 and Section 53 StPO.

119 French country report, Chapter III.B.3.

120 Croatian country report referring to Article 285 CPA; Estonian country report, § 72 Code of Criminal Procedure; Polish country report, Chapter III.B.3.; Dutch country report, Chapter III.B.3.

121 German country report, Chapter III.B.3.a. referring to Section 160a Subsection 1 Section 1 in connection with Section 53 StPO.

122 French country report, Chapter III.B.3. referring to Article 100-7 Penal Procedure Code.

123 UK country report, Chapter III.B.3. referring to Section 26(2) IPA.

counselling agency as well as their assistants and trainees.[124] In **France**, legislation protects judges and prosecutors from both interception and data capture by means of remote forensic software.[125] In **Switzerland**, according to statements by the participants of the law enforcement workshop, Article 170 Code of Criminal Procedure protects persons who have the right to refuse to testify for reasons of official secrecy. This includes public officials as well as members of authorities refusing to testify on secret matters communicated to them in their official capacity or which have come to their knowledge in the exercise of their office.

– *Exemption: no protection for professional secrecy in a case of suspicion*

The protection of professional secrecy in a criminal investigation does not provide absolute immunity against the interception of communications in any country included in the study. Several national reports – namely from **Austria**, **Belgium**, the **Czech Republic**, **Germany**, and **Spain**– indicated that an explicit exemption for such protection is provided in criminal procedure legislation if the person who is the subject of privilege is involved in criminal aid or criminal commission. Furthermore, in **France**, **Sweden**, and the **Netherlands**, although the rule on exemption in the case of suspicion is not directly provided for in the respective laws of criminal procedure, the interception of privileged communications is nevertheless possible under certain circumstances (in law and in practice).

In **Germany**, Section 160a Subsection 4 StPO stipulates that "when factual indications give rise to the suspicion that the protected person is involved with the offence being investigated, or participated in giving aid to the offender after the crime, in obstructing justice, or in dealing with stolen goods," no protection, whether conditional or unconditional, shall be given to this type of professional communication.[126] However, there is an exception: The suspicion of giving aid, obstructing justice, or dealing with stolen goods for the benefit of the suspect is insufficient for authorisation of interception of privileged communication between suspect and defence council. [127] In **Austria**, pursuant to the Section 157 Subsection 1 Nos. 2 to 4 StPO, a legal privilege applied to those who have the right to refuse to testify is no longer applied if the relevant persons are under strong suspicion of having committed an offence.[128] **Belgian** legislation provides for the possibility to authorise the interception of communications falling under professional privilege protection in cases in which the persons who are the subject of such pro-

---

[124] German country report, Chapter III.B.3.a. referring to Section 160a Subsection 3 in connection with Section 53a StPO.

[125] French country report, Chapter III.B.3. referring to Article 100-7 Penal Procedure Code.

[126] German country report, Chapter III.B.3.a.

[127] German country report, Chapter III.B.3.a.

[128] Austrian country report, Chapter III.B.3.

tection are suspected of committing or participating in the criminal offence allowing for the application of the interception of communications.[129] In the **Czech Republic**, an exemption from the special protection of communications between lawyer and defendant is possible if the interception is requested for investigation of a criminal act, which was "committed by the defence counsel in cooperation with the accused."[130] A similar provision exists in **Spain**, where the lawyer-client privilege does not apply if the counsel is involved in the offence with the suspect or defendant.[131]

The **Swedish** and **French** reports do not indicate that an exemption, such as a case of suspicion, is explicitly stipulated in the national law; however, in both countries, the interception of communications that are privileged is possible in criminal investigations. **Swedish** law provides for special circumstances in which people who enjoy professional secrecy protection can nevertheless be called upon as a witness, thus establishing exceptions from the general safeguards for privileged communications.[132] In **France**, the rules that prohibit the recording of privileged communications provide that interception is possible if the relevant professional associations are informed.[133]

– *Protection of the core area of privacy*

In addition to the protection of professional communications, there is a distinct model of protection for the "core area of privacy" against the interception of communications in **Germany**. Among the national legislations analysed in this study, only German law has established this type of special safeguard, provided for in Section 100d Subsection 1 StPO, against the interception of communications concerning the core area of privacy. The notion of the "core area of privacy," according to the German country report, refers to such types of information transfer as, e.g. the expression of "innermost feelings or expressions of sexuality." Unless there are serious indications that the information will reveal a direct link to the criminal act, special protection is given to the communications of a person where a particular relationship of trust in connection with the "core area" is concerned. As explained in the German country report, this type of communication encompasses such conversations as those with "close family members, priests, telephone pastors, criminal defence attorneys, or – in individual cases – doctors." In accordance with Section 100d Subsection 2 StPO, the consequence of this special protection is the

---

[129] Belgian country report, Chapter III.B.3.a. referring to Article 90*octies* Para. 1 and 2, 1° CCP.

[130] Czech country report, Chapter III.B.3.

[131] Spanish country report, Chapter III.B.3.a. referring to Article 118. 4. LECRIM.

[132] Swedish country report, Chapter III.B.2. referring to Article 27:22 CJP.

[133] French country report, Chapter III.B.3. referring to Article 100-7 Penal Procedure Code.

unconditional inadmissibility as evidence of communications related exclusively to the core area of privacy and the prohibition on interception of communications once it is revealed that the information exchange concerns the type of trust and intimacy that is the subject of this special protection. Any data related to the core area of privacy acquired during the course of interception must be immediately destroyed and cannot be used even as a mere clue in the criminal investigation.[134]

b) Privileged communications: practical implications and responsibilities for ensuring protection

While the analysis of legislation shows that at least certain types of professions (e.g. lawyers) enjoy special privileges against interception in almost every country, the way to ensure this protection in practice, both technically and procedurally, might vary from one jurisdiction to another even more than the law in books. This comparative analysis has identified several ways of dealing with interception in the national jurisdictions. The first two possible approaches are based on the deletion or blocking of the privileged content, while the third approach, by contrast, includes no obligation to make the content technically unavailable but implies that privileged communications, when intercepted, cannot be used in criminal proceedings.

The first approach identified *is interruption of interception, deletion of records, and filtering*. It can be found in the **Czech Republic**, **Germany**, **Hungary**, the **Netherlands**, **Sweden**, and **Switzerland**. The second way of dealing with privileged communications – *blocking the content but keeping the records* – exists in **Belgium**. The third approach, which does not require deletion of the intercepted content, but *prohibits using it in criminal proceedings*, has been adopted in **Australia**, **Austria**, **Estonia**, **France**, **Italy**, **Portugal**, and **Spain**. Further comparison will yield a detailed analysis of these approaches.

– *Interruption of interception, deletion of records, and filtering*

The first way of dealing with privileged communications in practice (identified in this study) is when interception of the privileged information must be discontinued, if done in real-time, and the records have to be deleted should any data have been acquired. This model is implemented in the **Czech Republic**, **Germany**, **Sweden**, and **Switzerland**. Furthermore, the **Netherlands** also follow this approach, but with the additional very distinct possibility of using special technology to filter the content of communications of persons covered by the lawyer-client privilege.

In **Germany**, the corresponding legislation requires a public prosecutor to already consider the protection of privileged communications and the core area of

---

[134] German country report, Chapter III.B.3.a.

privacy at the stage of application for judicial authorisation to intercept. Furthermore, the court must examine this issue when granting permission to intercept. If protected communication is nonetheless acquired, e.g. when the interception is carried out by means of automated recording without listening in real-time, the wiretapping must be stopped immediately, and records must be destroyed. This obligation has to be performed by an investigator in charge of the execution of the measure, with the possibility of consulting the public prosecutor, but only if this does not entail unnecessary delays concerning the requirement to destroy information. In all other cases, the decision on the introduction of the intercepted information in criminal proceedings lies with the public prosecutor.[135]

Similar to Germany, in **Sweden**, the person leading the criminal investigation is responsible for handling communications protected by the rules of legal privilege. Special safeguards are implemented to ensure that this power is not misused: if the decision about the protection of professional secrecy is unjustified, this can entail charges of the abuse of office.[136] When a person whose communication is intercepted is entitled to privilege, the law requires interrupting the ongoing interception immediately and destroying without delay all data obtained. The national reporter specifically highlights the fact that internet providers are not part of the process of assessment or blocking of privileged communications, since their duty is limited to capturing and transferring data in the process of interception; they have no power to determine what can be intercepted and handed over to law enforcement agencies.[137] Furthermore, since the interception of real-time monitoring is not possible in some cases of digital communication, the court is responsible for the final assessment of all data which were not deleted as irrelevant or privileged in conjunction with the issue of special protection.[138]

Another country requiring deletion of records of privileged communications is the **Czech Republic**. If such communication is captured during the performance of the interception, the police authority is required to delete the records without delay. Furthermore, the law prohibits using such information in the investigation. The destruction of such records shall be logged.[139] A similar approach was revealed with regard to the respective jurisdictions during the law enforcement workshops in **Hungary** and **Switzerland**.

A very interesting and distinct approach to interruption of interception and deletion of all records related to privileged communications can be found in the **Netherlands**. The Dutch model of dealing with the protection of professional secrecy in

---

135 German country report, Chapter III.B.3.b.

136 Swedish country report, Chapter III.B.2.

137 Ibid.

138 Ibid.

139 Czech country report, Chapter III.B.3. referring to Section 88 (1) Code of Criminal Procedure.

practice represents a hybrid model of deletion of records and filtering and deserves additional attention. As a general rule in the Netherlands, if the conversation of persons enjoying special privilege is recorded, it has to be deleted. However, this rule has different technical implications, depending on the profession in question. A specific technical solution is implemented for the communications of lawyers.[140] The special system, which holds all telephone and fax numbers used by lawyers in a filter registered with the National Interception Unit, was implemented in 2011. When the interception of communications starts, the traffic data are routed to this filter and, if the system recognises the number as belonging to a lawyer, the data capture ends automatically. If any delay in transfer occurs, any information already recorded is deleted. All lawyers in the Netherlands are obliged to register their telephone numbers in this system. However, this filtering rule is applicable, first of all, only to lawyers and, secondly, only to the content of voice (telephone) communications. Conversations of other professions pledged to confidentiality are not subject to this automatic filtering.[141] Automatic filtering is not performed for IP communications (IP traffic). There are ongoing discussions in the Netherlands on how to ensure the destruction of IP traffic because, although data can be deleted or overwritten, it is still technically possible to find them. All professional communications, such as those of medical professionals and clergymen, which are not automatically filtered, have to be deleted as soon as it is discovered that the communications fall under the non-disclosure rule.

– *Blocking content without deletion*

A second approach to dealing with the interception of privileged communications among the countries included in this study – making the acquired content unavailable but keeping the records – has only been adopted in **Belgium** due to very specific concerns about the integrity of the evidence. As was revealed at a workshop with Belgian law enforcement agency representatives, the investigators who analyse the intercepted content must issue a notification that a particular communication falls under this privilege and request to have it secured so that no one besides the National Tech Support Unit and the court can access the communications without credentials, such as password. The content is not deleted, but it is technically hidden and protected after analysis of the intercepted material. Investigators in Belgium always have to go through all the acquired content before issuing a notification about protected communications, because criminals can use tricks, e.g. pretending that they are communicating with a lawyer. As a measure of privacy protection, the judge issues an order to appoint a police officer responsible for the

---

[140] See Dutch country report, Chapter III.B.3. For more details, see, *Odinot* et al., Summary – The use of telephone and Internet taps in criminal investigations, 2012, available at: https://english.wodc.nl/onderzoeksdatabase/effectiviteit-van-tappen.aspx?cp=45&cs=6798 [last accessed 04/2020].

[141] Ibid.

selection of the conversations. The right to privacy guarantees that, if the conversation is not related to the investigation or concerns private life (e.g. sexual activities), the officer is allowed to listen to it but has to mark the conversation as irrelevant. This conversation can be further "unpacked" during the proceedings if there is any controversy about its content with regard to what was selected. Previously, there was no possibility to remove irrelevant conversations; however, after Belgium decided to separate the information related to the investigation from other information, the police have to write down what is removed so there is always a possibility for review. No content needs to be deleted and filtered, since the defence lawyers can question the integrity of the records. Furthermore, the Belgian country report noted that judicial practice reinforces the necessity of retaining the records even if the interception is nullified: In a judgment of 18 February 2003, the Supreme Court of Belgium decided that the right to defence justifies access by the defence to the documents resulting from investigation measures that have been declared nullified.[142] Thus, all the records are retained in a special registry allowing for access under certain conditions.

– *No obligation to delete, but the information cannot be used*

In some jurisdictions, such as in **Australia, Austria**, **Estonia**, **France**, **Italy**, **Portugal**, and **Spain**, the content is neither deleted nor blocked. In **Austria**, as was stated by participants during the respective workshop with law enforcement personnel, the information is intercepted from time to time, and the prosecutor has to decide what can and cannot be used as evidence if such privileged communication is recorded. In accordance with **Australian** legislation, communication that is accorded privileged status cannot be used as evidence.[143] **Italian** police forward information to the prosecutor, who then decides what can and cannot be used; the recordings can be destroyed only after conclusion of the investigation and judicial proceedings.[144]

In **France**, when the interception of privileged communications is taken into consideration in a criminal investigation, the law requires an application for consent from the respective professional associations before the measure can be authorised. This responsibility is the duty of a judge who grants permission to perform the interception.[145] In general, the police can use only communications related to the purpose of the investigation. As stated by law enforcement agency representatives at the workshop, in France, privileged information is considered irrelevant to the investigation.

---

[142] Belgian country report, Chapter III.B.3.b. referring to Supreme Court, 18 February 2003, P.02.0913.N.

[143] Australian country report, Chapter III.B.3.

[144] Italian country report, Chapter III.B.3.

[145] French country report, Chapter III.B.3.

In **Spain**, the protection of privileged communications is a duty of the court and not of the police performing the interception; thus, the content is neither deleted nor blocked before it goes to court. Furthermore, special limitations on the interception of communications between a suspect and a defence lawyer provide that such content will not be used in court, despite having been acquired in practice during the course of an interception.[146] Both the Spanish national report and the law enforcement workshop in Spain revealed that the law there provides no model for dealing with such situations: the police have to record all data during an interception because they technically and legally do not have the capacity to remove this privileged communication. Therefore, all communication content is recorded and the police have to make transcripts, which also include privileged communications. Nothing can be removed from the transcript because the police may not manipulate the evidence. It is the duty of a judge to ensure special protection of privileged communications.[147] The judge has to decide what has to be removed if the intercepted material contains privileged communications when he/she receives the transcript; thus, investigators are not responsible for handling the issue of professional secrecy. Privileged communications, however, cannot be presented as evidence in court. The new regulation on the interception of communications, adopted in 2015, has not essentially changed this approach and has not outlined any new procedures in the handling of privileged communications, leaving it to the judge to order parts of the conversation containing professional secrecy removed.[148]

In the **United Kingdom**, the intercepted material can generally not be used in court (unless there exist exceptional circumstances);[149] thus, safeguards concerning the deletion of data falling under legal privilege are not as relevant as in those countries where interception can be used as evidence in criminal proceedings.

4. Execution of telecommunications interception

a) Interception via communications providers and interception with the use of LEA-own equipment

In all of the countries included in this study, the standard mode of interception is to order telecommunications service providers to extract data and surrender it to the law enforcement agencies. However, despite the existence of a general regime to carry out interception by means of orders submitted to the telecommunications providers, many national reporters indicated that law enforcement agencies are allowed to use their own equipment to perform the interception.

---

146 Spanish country report, Chapter III.B.3.a.

147 Ibid.

148 Spanish country report, Chapter III.B.3.a. and information obtained at law enforcement workshop.

149 See, UK country report, Chapter IV.

The **German** report states that "according to prevailing opinion, the law enforcement authorities are permitted to perform the interception by their own means,[150] for instance by gaining access to a wireless network."[151] Similarly, the **Belgian** national reporter points out that the main interception provision in Article 90*ter*, 1° and 2° CCP does not impose any direct requirement on law enforcement agencies to cooperate with third parties while performing the interception, thus allowing for the use of their own technical tools, if necessary.[152] The **Swedish** national report, while highlighting that law enforcement agencies can use their own equipment without relying on service providers to execute the interception, additionally addresses the question of direct access of law enforcement agencies to cables or other parts of telecommunications infrastructure. Access to the signal bearers, such as fibre-optic cables, without participation of the communications providers is permitted in Sweden only in the case of signals intelligence collection and cannot be used in criminal investigations.[153] The **Croatian** report points out that, though law enforcement authorities are allowed to use their own tools to perform an interception, most of the interceptions require cooperation with providers.[154] Similar information was shared by the law enforcement personnel at the workshop in **Hungary**: while the law does not forbid the use of the police's own tools, the police mostly lack both the tools and expertise to take advantage of this.

Some country reports indicated that the police's use of their own tools is to be provided for in the interception warrant. In **Spain**, the use of special equipment, though permitted, has to be indicated in the interception authorisation. This is due to the fact that lawful interception can be carried out only under the conditions provided for in the court order; the use of any equipment that is not part of the centralised system has to be authorised by the court and explained to the judge who granted authorisation.[155]

b) Accompanying investigative powers

In addition to the interception of communications, the national law can allow for the use of different accompanying investigative powers, such as clandestine access to houses in order to install equipment, hacking techniques, the use of key loggers, etc. One of the major current issues and, at the same time, a source of divergence, is the problem of the use of remote forensic software.

The use of remote forensic software will be discussed in detail in a special chapter on this topic (Chapter III.D.1.). Suffice it to briefly mention here that

---

150 German country report, Chapter III.B.4.a.

151 Ibid.

152 Belgian country report, Chapter III.B.4.a.

153 Swedish country report, Chapter III.B.3.

154 Croatian country report, Chapter III.B.4.

155 Information obtained during the law enforcement workshop.

such use is explicitly permitted in the laws of several countries: **Australia**, **Austria**, **France**, **Germany**, **Italy**, the **Netherlands**, **Spain**, **Switzerland**, and the **United Kingdom**. Other national reports noted the lack of powers concerning such an investigative measure in their respective laws on criminal procedure. The approaches to this issue in the absence of explicitly provided powers vary from country to country. In the **Czech Republic** and **Portugal**, the use of remote forensic software might be legally permissible. However, the Czech Republic has no experience in the application of general provisions to the use of such software. In **Sweden**, the law requires physical installation of the remote forensic software. Further analysis as to details and justification for the use of remote forensic software can be found in this study in Chapter III.D.1.

5. Duties of telecommunications service providers to cooperate

With the development of information and communication networks, which today include various applications and services, the duty of communications providers to cooperate in the interception of communications poses serious challenges for criminal investigations. The duty of cooperation for the purpose of interception of communications is twofold and applies, first, to the communication providers who are subject to telecommunications regulation, and, secondly, to the unregulated entities providing other services related to data transmission. The first type of relationship between law enforcement and communication providers is fairly straightforward as far as the duty to cooperate is concerned. The communications service providers that fall under the scope of telecommunications or electronic communications regulation are commonly subjected to such a duty. They are normally obliged to make communications transmitted through their networks available for interception and provide intercepted data to law enforcement agencies in a readable format.

Nowadays, however, it is not only communications providers falling under the scope of regulation of electronic communications who can transmit information that might be of importance for criminal investigations and needs to be intercepted. The traditional scope of the obligation of interceptability for networks and services does not cover all existing communication and service providers in a sufficient manner. With the development of Voice-over-IP communications, as well as different messengers and chat applications that can be either integrated into social networks and other services or exist as mobile phone applications, the possibilities for communications transmissions are endless. In many cases, the scope of the "traditional" specific provisions on the duty of communications providers to cooperate cannot adequately cover the new applications and services, not only because many providers are outside the scope of specific duties but also simply because they are not physically present on a country's territory and thus cannot be forced to cooperate even under more general provisions on assistance in criminal investigations.

In most of the countries, the duty to cooperate is provided for either in the rules of criminal procedure, in a special communications regulation, or both. However, when it comes to providers who are not physically present on the national territory or do not fall under the communications regulation, the national law does not fully solve the problem. While some of the countries allow for a broader interpretation of the provisions on the duty to cooperate, others limit them to only regulated entities, such as telecommunication providers or internet service providers. The following analysis covers three aspects of this issue: first, it examines specific legislation related to cooperation between communication service providers and law enforcement agencies; secondly, it considers the scope of the provisions with regard to the entities falling under the duty to cooperate; and, thirdly, it discusses the problems of limitation of current legislation.

– *Specific legislation on the duty to cooperate*

There are several ways to implement the duty of service providers to cooperate on interception in criminal investigations in the national legislation. It can be provided for either in rules of criminal procedure or in a special communications regulation, or both.

Austria, the **Czech Republic**, **Germany**, **France**, **Hungary**, the **Netherlands**, and **Poland** address the issue of providing assistance for the purpose of interception by outlining the general duty to cooperate in a criminal investigation in the law of criminal procedure *and* by using the special telecommunications legislation. In **Germany**, Section 100a Subsection 4 StPO obliges anyone providing, or contributing to the provision of, telecommunication services on a commercial basis to assist the public prosecutor's office in implementing any measures required for the interception/recording of the communication and to supply all necessary information without delay.[156] The measures referred to in the above-mentioned provision are further detailed in the Telecommunications Act (TKG), the Telecommunications Interception Ordinance (TKÜV), and the associated technical guidelines (TR TKÜV). Similarly, in **Austria**, Section 138 Subsection 2 StPO provides for the general duty of service providers to provide information and assist investigations, while Section 94 TKG 2003 sets out comprehensive cooperation duties for providers.[157] In the **Czech Republic**, the duty to cooperate falls under a general provision – Section 8 Code of Criminal Procedure –, which obliges any natural or legal person to comply with requests from law enforcement agencies.[158] Furthermore, the Czech Act on Electronic Communications requires any entities involved in the provision of a public communication network or a publicly available electronic com-

---

156 German country report, Chapter III.B.5.a.

157 Austrian country report, Chapter III.B.5.

158 Czech country report, Chapter III.B.5.a.

munication service to make their networks interceptable and to provide assistance in the execution of the interception. **French** legislation follows the same approach, providing for a general duty of every citizen to comply with lawful requests from law enforcement entities and courts,[159] detailing some specific rules in the French Post and Communications Code.[160] In the **Netherlands**, a duty to cooperate is stipulated in Article 13.2 of the Telecommunications Act, which requires providers of public telecommunication networks to provide assistance, while the Dutch Code of Criminal Code also contains several specific provisions related to this requirement.[161]

Several countries included in this study – **Australia**, **Sweden**, and the **United States** – detail the duty to cooperate in special, mostly telecommunications-specific legislation. In **Sweden**, the Electronic Communications Act and special ordinances stipulate the duty of any regulated providers of electronic communication services to cooperate with law enforcement agencies for the purpose of the interception of communications.[162] In **Australia**, the framework for cooperation is established in the Section 313 of the Telecommunications Act; however, further provisions on the duty to cooperate can be found in specific legislation related to interception – namely the TIA Act.[163] The **United States** enacted the Communications Assistance for Law Enforcement Act of 1994, which outlines the duties of communication providers with regard to cooperation in the interception of communications.[164]

The legislation in **Belgium**, **Croatia**, **Italy**, **Spain**, and the **United Kingdom** provides for the duty to cooperate in the interception-related provisions of the law of criminal procedure. For example, in **Belgium**, the provisions of Article 90*quater* Para. 2, 4 Code of Criminal Procedure require natural and legal persons to cooperate in the interception of communications. **Spanish** procedural law also features a broad scope for the duty to cooperate in the performance of interception: Article 588*ter* LECRIM obliges any telecommunication service provider and any persons playing a role in facilitating communications to comply with cooperation orders from a judge, public prosecutor, and the police during the course of the execution of communications interception.[165] The **Croatian** report pointed out that other than few general provisions such as power to intercept and duties to cooperate, the full range of the obligations falling under such duty is not detailed in legislation, nor is otherwise disclosed to the public.[166]

---

159 French country report, Chapter III.B.5. referring to Article 10 Civil Code.

160 French country report, Chapter III.B.5.

161 Dutch country report, Chapter III.B.5.

162 Swedish country report, Chapter III.B.4.

163 Australian country report, Chapter III.B.5

164 USA country report.

165 Spanish country report, Chapter III.B.5.a.

166 Croatian country report, Chapter III.B.5.a.

– *The subjects of the duty to cooperate*

The scope of legal rules that oblige communication providers to cooperate with law enforcement agencies for the purpose of interception of communications is one of the most prevailing and controversial issues, as was pointed out during several workshops with law enforcement agencies during the data collection phase of this study. All of the countries included in this study have legislation requiring "traditional" communications providers to make communications transmitted through their networks interceptable. However, with the development of different applications and services, the interception of many types of communications passing through various devices and networks is difficult, if not impossible, because most of the national laws have their limitations with regard to which entities are regulated or can be forced to cooperate.

Some of the countries, like **Croatia**, the **Czech Republic**, **France**, the **Netherlands**, and **Sweden** instead limit the duty to cooperate in interception to only the entities that are the subject of telecommunication regulation. In the **Czech Republic**, only providers of a network infrastructure or an electronic communications service, which have a license issued by the Czech Telecommunications Office, fall under this obligation. Providers of information society services, e.g. cloud providers, social networks, e-mail service providers, portals, and search engines are not obliged to cooperate for the purpose of communications interception.[167] In **France**, as is highlighted in the national report, according to the French Post and Communications Code, the entities that are subject of the obligation to cooperate are electronic communications operators and internet access providers.[168] In the **Netherlands**, Article 13.2 of the Telecommunications Act requires only public telecommunications network providers to cooperate.[169] **Croatian** legislation refers only to "operators of public communication networks" and "publicly available electronic communication services."[170] Similarly, in **Sweden**, Section 6:19 of the Electronic Communications Act refers only to "telecommunication services" when it establishes the duty to provide data in an accessible form.[171] Swedish law enforcement representatives during the workshop confirmed that only those services

---

[167] Czech country report, Chapter III.B.5.a.

[168] As the French country report (Chapter III.B.5.) points out, the electronic communications operators are defined in Article L.32, 15° Post and Electronic Communications Code as "natural or legal persons who exploit an electronic communications network opened to the public or who provide the public with an electronic communications service" (the notion of "provision" being understood here as the transmission of electronic communications on a network). Internet access providers are defined in Article 6, I, 1 of Law 2004-575 of 21 June 2004 as "persons whose activity is to provide an access to online public communication services."

[169] Dutch country report, Chapter III.B.5.

[170] Croatian country report Chapter III.B.5.

[171] Swedish country report, Chapter III.B.4.

provided by regulated telecommunication companies are considered "communication services."

Other countries, like **Australia**, **Austria**, **Belgium**, **Germany**, **Spain**, and **Switzerland**, interpret the provisions on the duty to cooperate in a broader way. In **Germany**, the TKG provides that the term telecommunications services comprises those services consisting wholly or mainly in the conveyance of signals through the telecommunications networks.[172] As explained in the German country report, this definition includes mainly access providers and network providers providing services to the public;[173] however, a broader interpretation basically allows for the inclusion of e-mail services, as long as the focus of the service is the transmission of data. In addition, access providers who do not provide an identifier for monitoring purposes but are involved in the transmission of communications may also possibly be subjected to this duty.

The **Austrian** country report points out that pursuant to Section 134 (3) StPO, a surveillance of messages and information can be carried out not only on communications networks, but also on information society services.[174] In **Belgium**, the scope of the duty to cooperate is quite broad and, according to the national reporter, includes "infrastructure providers working on the IP-transport level (operators of a telecommunications network), Internet Access Providers (IAP's) and Internet Service Providers (ISPs), such as social media providers and cloud computing service providers."[175] Belgian judicial practice also reveals that the duty to cooperate might be interpreted much more broadly for regulated communications providers: e.g. the Belgian Supreme Court, in its decision of 18 January 2011, used a broad interpretation of the term "electronic communications provider" for the purpose of Article 46*bis* CCP, covering e-mail providers.[176] **Spanish** procedural law also features a broad scope for the duty to cooperate in the performance of the interception: Article 588*ter* LECRIM obliges any telecommunications service provider and any persons playing a role in facilitating communications to comply with cooperation orders from a judge, public prosecutor, and police during the course of the execution of communications interception.[177]

Furthermore, some countries, like **Australia**, amended their legislation to include a broader interpretation of the subjects of the duty to cooperate. Australia amended its Telecommunications Act in December 2018 to introduce the concept

---

[172] *Vodafone*, Law Enforcement Disclosure Report, Legal Annexe, June 2014.

[173] Other than regulations in the TKG, Section 100s Subsection 4 StPO also generally covers not only public telecommunication systems but also closed communication networks, such as corporate networks. See, German country report, Chapter III.B.5.a.

[174] Austrian country report, Chapter III.B.2.

[175] Belgian country report, Chapter III.B.5.a.

[176] Belgian country report, Chapters III.B.5. and C.b.

[177] Spanish country report, Chapter III.B.5.a.

of a 'designated communications provider.' The definition of designated communications provider includes a broader range of service providers, including foreign and domestic communications providers and device manufacturers.[178] The same path was taken in **Switzerland**: at the law enforcement workshop, participants revealed that new regulation, which entered in force in March 2018, introduced a duty to cooperate for approximately 500 providers of communications services (previously, the number was 50) and now covers multi-way communications, such as Google Docs.

– *Current debates*

Even if national legislation on the duty to cooperate, e.g. in Belgium, allows for a broader interpretation of the term "communications provider" or is general enough to oblige any entity to comply with the interception request, the enforceability of such provisions is not always straightforward if the provider of a particular service is outside of the reach of law enforcement agencies due to jurisdictional issues. As shared by the representatives of national law enforcement agencies during the workshop phase of this study, it is difficult, if not impossible, to intercept communications when they are transmitted via messengers or a few Voice-over-IP services, if the service providers use encryption and are not physically present in the particular jurisdiction.

There are different suggestions on how to solve these problems, but all of them raise more questions than provide answers. For example, calls to extend the telecommunication regulation to cover the providers of messenger or Voice-over-IP services might raise the issue of the actual incompatibility of such services with the traditional notion of communications providers and could require reconsideration of the entire concept of the communication infrastructure, networks, and services. A simple extension of the general duty to cooperate in interception matters to these services also would not solve the problem as long as the issue of enforceability of such provisions in foreign jurisdictions is not addressed. It is outside the scope of this study to analyse different possible solutions to the problem of the duty of providers to cooperate in the interception of communications. With the continued development of information technologies, services, and applications, however, these issues will require attention. Future solutions might require not only national legal reforms but also better international cooperation and coordination.

---

[178] Australian country report, Chapter III.B.5.

6. Formal prerequisites of interception orders

a) Competent authorities

In all the countries included in this study, with the exception of the **United Kingdom**, an interception is normally authorised by the court upon the request of either a police officer or – in most of the countries – a prosecutor. In the **United Kingdom**, there exists a double-lock procedure: the Secretary of State (or the Scottish Ministers in the context of a Scottish application) has the authority to issue interception warrants; however, the Secretary of State may not – except in urgent cases – issue a warrant without this decision having been approved by a Judicial Commissioner.[179] Some exceptions from the rule of prior court authorisation are possible in most of the countries; prominent among these exceptions, as will be analysed further, are applications for interception in urgent circumstances.

The formal prerequisites for granting interception authorisation, however, may vary for both obtaining the warrant under normal circumstances and authorising the interception in urgent situations as regards who the competent authority is and how to apply for permission to intercept. In **Australia**, **Austria**, **Croatia**, the **Czech Republic**, **Germany**, **Italy**, the **Netherlands**, **Poland**, **Portugal**, **Spain**, **Sweden**, and **Switzerland**, interception is authorised by the court upon application of either the prosecutor or the police; in **Belgium** and **France**, the investigating judge can authorise interception in his or her own investigation. Concerning urgent circumstances, further divergences can be found with regard to how the interception is authorised in cases of emergency. The differences at the national level are outlined in the following analysis: firstly, part (aa) will consider authorisation in normal situations and, secondly, part (bb) will follow with an analysis of applications for urgent warrants.

aa) Authorisation in normal situations

– *Authorisation upon prosecutor's or police officer's application*

Most of the countries included in this study – **Australia**, **Croatia**, the **Czech Republic**, **Estonia**, **Germany**, **Hungary**, **Portugal**, and **Sweden** – have a model of authorisation in which the public prosecutor or a police officer apply for the judicial authorisation.[180] The **Czech** and **Swedish** reports indicated that prosecutors

---

[179] UK country report, Chapter III.B.6.

[180] Australian country report, Chapter III.B.6.; Croatian country report, Chapter III.B.6.; Czech country report, Chapter III.B.6.a.; Estonian country report, Chapter III.C.4.; German country report, Chapter III.B.6.a. referring to Section 100a StPO; Hungarian country report, Chapter III.B.6.; Portuguese country report, Chapter III.B.; Swedish country report, Chapter III.B.5.

closely collaborate with the police to file such an application.[181] In the **Netherlands**, **Austria**, and **Switzerland**, while court approval is required, the role of the prosecutor is different: it is the prosecutor who authorises, orders, or starts interception, and the court confirms it.[182] In **Spain**, while judicial authorisation is necessary, both police and prosecutor are competent to submit an application for judicial authorisation on their own. As stated in the Spanish country report, a judge can also apply for the interception *ex officio*.[183]

In the **United States**, authorisation differs on the federal level and state level. At the federal level, to secure a valid interception order in a federal criminal investigation, a senior U.S. Department of Justice official must approve the application for the court order. However, any federal prosecutor may approve an application for court authorisation for real-time interception of e-mail or other electronic communications. At the state level, the application to the court for wiretapping or electronic eavesdropping can be made by the highest prosecutor in each state or any of its political subdivisions.[184]

– *Mixed model of court authorisation*

Belgium and **France** have a mixed model of issuing authorisation for the interception of communications due to the existence of the institution of the investigating judge. In **Belgium**, authorisation is an issue for consideration by the investigating judge,[185] but the process of authorisation depends on the body actually investigating the offence. The first possibility for the authorisation consists of the police requesting that a prosecutor apply for the interception, which is then granted by a judge. However, as was revealed during the law enforcement workshop in Belgium, the existence of an investigating judge provides for the second option, where the judge who takes over the investigation of the criminal case can authorise interception for the purpose of investigation in his own capacity. Cases in which a public prosecutor is not involved in the process of authorisation also include situations in which another identifier (e.g. a second telephone number) is discovered during the same investigation. Under the Belgian system, when a public prosecutor considers cases that need interception and transfers the file to the investigating judge together with a request to investigate, the judge has to examine the case within this requisition. Thus, the power of the judge is limited to the crimes ordered for investigation in the requisition, and there is no possibility to go outside the borders

---

[181] Czech country report, Chapter III.B.6.a.; Swedish country report, Chapter III.B.5.

[182] Austrian country report, Chapter III.B.6.; Dutch country report, Chapter III.B.6.; Switzerland: information obtained at the law enforcement workshop.

[183] Information from Spanish country report, Chapter III.B.6.a. and from Spanish law enforcement workshop.

[184] USA country report

[185] Belgian country report, Chapter III.B.6.a. referring to Article 90*ter* Para. 1 CCP.

of the investigation of a particular case. Yet, since the duty of an investigating judge is to find the truth via all possible means, he/she can therefore order the interception without the police and prosecutor being involved in the authorisation process if this investigative measure falls within the framework of the requisition. Consequently, in some cases, there is no application for interception but only an order issued by a judge.

A complex model for interception authorisation exists in **France**, depending on the type of the crime and other factors. In general, based on Articles 100 to 100-7 PPC, interception may be ordered by the investigating judge for the investigation of felonies and misdemeanours where the penalty incurred is equal to or in excess of two years' imprisonment, or to search for the cause of death or disappearance of a person. Furthermore, the liberty and custody judge of the District Court may, when the requirements of the investigation call for it, upon request by the district prosecutor, order a correspondence intercept to facilitate the search for a fugitive. Finally, in relation to certain organised crime cases, the liberty and custody judge of the District Court may also order a correspondence interception, upon request by the district prosecutor.[186]

– *Authorisation by the Judicial Commissioner*

The **United Kingdom** is the only country among those included in this study where the warrant to intercept has to be approved not by a court, but by a judicial commissioner.[187] The relevant provision was introduced by the IPA in 2016. Previously, no judicial approval was required.

bb) Interception in urgent circumstances

The cases of emergency in all of the countries included in this study represent an exemption from the normal process of granting authorisation for interception in order to enable law enforcement to start interception as quickly as possible. These exemptions differ, however, with regard to how the applications in urgent situations are *addressed* in the law of criminal procedure and/or in practice. There are two possible approaches to cases of emergency. Firstly, in most of the countries, the law of criminal procedure outlines a special procedure for such situations. Secondly, when the law does not address this issue, as in the **Czech Republic**, **France**, and **Portugal**, special procedures have been developed in practice by the police, prosecutors, and courts to solve the problem of urgent authorisation and issuing the court warrant as quickly as possible. The two approaches are analysed further in this chapter.

---

186 French country report, Chapter III.B.6.

187 UK country report, Chapter III.B.6.

– *Urgent warrants with no court authorisation or with subsequent court approval*

The special procedures to start interception in urgent circumstances via an order by the prosecutor, with subsequent court approval, are provided for in the law of criminal procedure of **Croatia**, **Germany**, **Hungary**, **Italy**, the **Netherlands**, **Poland**, **Spain**, and **Sweden**. In **Switzerland**, where the court approves interception subsequently within five days after the prosecutor starts it, the situations of emergency follow the same procedure as a regular interception in terms of court approval.[188]

German law of criminal procedure, e.g. stipulates that, when urgency requires the interception of communications for the purpose of criminal investigation, the public prosecutor's office is empowered to issue an interception authorisation, which must further be approved by the court within three working days after the date of issue. If the authorisation is not subsequently judicially approved, it becomes ineffective.[189] The same approach is found in **Swedish** legislation, which was amended in 2014 to address the issue of interception in urgent cases. This amendment grants a prosecutor the power to temporarily authorise interception in emergency circumstances, providing that the reasons for the decision are stated and the issue of authorisation is forwarded to a responsible judge, who can confirm or revoke the interception order without delay.[190] As noted in the Swedish report, before the amendment was introduced in 2014, the emergency procedure was provided only for certain types of crimes against national security and, therefore, rarely used in practice, e.g. it was ordered only four times from 2009–2012.[191]

In **Australia**, **Austria**, **Estonia**, and the **Netherlands**, warrants to intercept can be granted via telephone;[192] **Belgian** law also allows for a verbal approval.[193] Furthermore, in **Estonia**, e-mail or other means of communications, such as text messages, can be used for urgent authorisations, as well.[194] Further divergences can be found in **Spanish** legislation. The emergency warrant can be granted under very limited circumstances. This urgent procedure for starting interception without judicial authorisation does not involve the prosecutor as a competent authority and gives the power to grant interception to administrative governmental bodies. Emergency procedures can be used only in case of terrorist crime, and it is the Ministry of Interior or the Director of State Security that has the power to issue the warrant. The court must subsequently be informed within 72 hours in order to revoke or

---

188 Information obtained at the law enforcement workshop.

189 German country report, Chapter III.B.8.a. referring to Section 100b(1) StPO.

190 Swedish country report, Chapter III.B.5.

191 Ibid.

192 Australian country report, Chapter III.B.6.; Austria: information was obtained during the workshop with law enforcement; Dutch country report, Chapter III.B.6.

193 Belgian country report, Chapter III.B.6.c. referring to Article 90*quater* CCP.

194 Information from the workshop with Estonian law enforcement agencies.

confirm the interception.[195] Up to the adoption of new legislation in 2015, the same power was provided for in Section 3 of Article 579 Criminal Procedure Act. However, according to the Spanish law enforcement representatives, this possibility had never been used in practice. In emergency cases, the police and the prosecutor can obtain a warrant from the judge on duty within approximately four hours.[196]

– *No special procedure for urgent warrants*

Another approach is taken by those countries where the possibility to intercept without a court warrant in urgent circumstances is not provided for in their respective laws. These countries, namely the **Czech Republic**, **France**, and **Portugal**, have developed certain procedures in practice to address the emergency situation and quickly obtain court authorisation in writing.

For example, in the **Czech Republic**, the law in fact provides for a few exceptions whereby the interception can be carried without a warrant for serious crimes. However, the exceptions in cases of urgent interception listed in Section 88 (5) of the Czech Code of Criminal Procedure require the consent of one of the parties of the intercepted communication. These cases concern such criminal acts as human trafficking, certain types of kidnapping, etc.[197] In any other urgent cases, or in a situation in which a party to the communications does not consent to the interception, the process of interception authorisation strictly follows the normal procedure of obtaining a court warrant. However, as Czech law enforcement agency representatives explained during the workshop, there are procedures to allow the authorisation to be obtained quickly: in urgent cases, there are judges and prosecutors on duty who can be reached 24 hours/7 days a week. Police investigators also have the option of submitting an urgent application for interception authorisation. Furthermore, there is always a person on duty in the interception unit to handle interception orders issued at night.

Similarly, a procedure to obtain a court authorisation quickly was adopted in **France**, where the law requires written warrants to be issued in any case, even in urgent matters. As French law enforcement representatives revealed during the workshop, there is a special procedure for emergency cases, when the crime is serious, and the investigation calls for immediate action. If an enquiry or a preliminary investigation is needed for one of the offences falling under the scope of Article 706-73 of the French Penal Code (which contains a list of serious crimes, such as organised crime, drug trafficking, kidnapping, etc.), the prosecutor can request urgent authorisation of the interception of communications.[198] The judge of liberty

---

[195] Spanish country report, Chapter III.B.6.a. referring to Article 588*ter* c. LECRIM.

[196] Information obtained at the law enforcement workshop.

[197] Czech country report, Chapter III.B.7.f.

[198] Article 706-95 Penal Procedure Code.

(juge des libertés et de la détention) can grant this authorisation for a maximum period of one month, and the decision of the judge must be issued in written form. In practice, the situation can be resolved on the phone, with the judge sending the decision in writing, which takes approximately 30 minutes. Each court has a judge on duty to handle such cases. Communication providers do not start intercepting without this decision, but the authorisation is usually submitted to telecommunication providers by fax or e-mail to speed up the process in urgent cases.

b) Formal requirements for applications

The law of criminal procedure and other regulations can establish formal requirements that are to be met in applications for the interception warrant, e.g. written form or the necessity for an oral hearing. Such provisions can be found in the law of criminal procedure of some of the countries, such as **Spain** and **Sweden**. Other countries have no requirements outlined in the law but, e.g. in the case of the **Czech Republic**, there are special regulations, such as a code of practice or binding guidelines.

– *No formal requirements outlined in the law of criminal procedure*

No special requirements for interception applications exist in **Austria**, **Croatia**, **France**, **Germany**, and in **Italy**. However, in practice in **Germany**, there are still substantial prerequisites for the submission of such an application: as pointed out in the German country report, a prosecutor cannot submit a request that merely sums up the circumstances of the case, because the court has a duty to assess all the necessary prerequisites for ordering the investigative measure. It is therefore necessary for the public prosecutor to present all the relevant evidence determining the need for the interception, together with the investigative file, if the case is complex.[199] In **France**, criminal procedure law does not impose any specific requirements. The French national reporter expressly notes that the form of the interception application is neither regulated nor outlined in the law of criminal procedure.[200] The academic report from France, as well as the practical workshop, revealed that no specific regulation exists concerning formal requirements for the application.

– *Formal requirements outlined in the law of criminal procedure*

In the **Netherlands**, **Spain**, and **Sweden**, some of the formal prerequisites are provided for in the law of criminal procedure. The **Dutch** country report states that Para. 2 of Article 126m Code of Criminal Procedure describes the formal requirements that should be met regarding the text of an order, to meet the legal stand-

---

[199] German country report, Chapter III.B.6.b.

[200] French country report, Chapter III.B.6.b.

ards.[201] Similarly, **Spanish** law outlines a detailed set of requirements regarding application for the authorisation of interception of communications: the applications must contain a description of facts, among them a detailed statement justifying the application of the measure, the form of execution, the necessary duration, and identifiers concerning the person and connection, to name but a few.[202]

In comparison to Spain, the law in **Sweden** outlines different mandatory requirements for the interception requests: firstly, the application must be made in writing and, secondly, any related oral hearings must be documented.[203] The application for interception is not made on oath; however, it is safeguarded by the threat of conviction for misuse of office in cases of negligent applications. As stated in the Swedish report, such cases of conviction for misuse of office have taken place in practice: For example, in 2000, a prosecutor faced criminal charges for submitting a negligent application for interception authorisation because the legal requirements for ordering this measure had not been met.[204] A general procedure used in Sweden is to consider the request for interception at the court hearing, with both a police investigator and a public prosecutor present in person. As was stated at the workshop with Swedish law enforcement agency representatives, in practice, this hearing is always a discussion in person, despite the fact that there is no legal requirement for a personal meeting. When it is not feasible to travel to the court – e.g. if the court is situated in a remote location – the prosecutor and the judge can arrange a videoconference, or the prosecutor and the police can ask colleagues to represent them at the court hearings. It is impossible to just send a request with a report if secret wiretapping is concerned: a personal meeting is always required in practice. In addition, the Swedish system provides for the institution of public representatives, who must be present at the interception application hearings. The representative is usually a retired judge or a lawyer representing public interests. This is an additional safeguard: the public representative is considered to be an ombudsman.

– *Formal requirements outlined in other regulations*

While the laws in the **Czech Republic** contain no specific requirements for the application for interception, they are outlined in a different piece of regulation. The **Czech** national report refers to Article 67 of the binding guideline No. 30/2009 Sb.

---

201 Dutch country report, Chapter III.B.6.

202 Spanish report, Chapter III.B.6.b. referring to Article 588*bis* b. 2) and Article 588*ter* d. LECRIM. A detailed list of formal requirements can be found in the Spanish country report in the respective chapter on the formal requirements of an application for interception.

203 Swedish country report, Chapter III.B.5., referring to Article 21 Code of Criminal Procedure.

204 Swedish country report, Chapter III.B.5.

on the tasks in criminal proceedings,[205] which establishes formal prerequisites for a request for interception of communications, providing that it must contain information such as specific facts about the case, a description of the offence, identifiers for the purpose of interception, and other data.[206]

c) Formal requirements for interception orders

In addition to demanding the warrant application to be made in a specific form, the law of criminal procedure can establish formal requirements for interception warrants. All the countries included in this study require the authorisation to be made in writing, except authorisation granted in urgent circumstances, e.g. telephone authorisation in **Australia** or the **Netherlands**.

In addition to the written form, specific formal requirements in most of the countries refer to identification for the interception (either name, number, or terminal device), e.g. in **Austria**, **Belgium**, the **Czech Republic**, **Germany**, and **Spain**.[207] The obligation to mention the type and duration of the measure represents yet another formal requirement established in all of the countries' procedural law.[208] In **Austria**, **Belgium**, the **Czech Republic**, **Germany**, and **Spain**,[209] legislation requires that the warrant give the reasons justifying the interception.

7. Substantive prerequisites of interception orders

Since the interception of communications represents one of the most intrusive investigative measures, as it conflicts with the individual's right to privacy, most of the national legislations on interception have established sets of checks and safeguards in order to ensure that interception takes place only when necessary and that

---

[205] Czech country report, Chapter III.B.6.b. referring to binding guideline No. 30/2009 Sb., on the tasks in criminal proceedings.

[206] Czech country report, Chapter III.B.6.b.

[207] See respective country reports referring to Section 100e Subsection 3 StPO (German country report, Chapter III.B.6.c.); Article 90*quater* CCP (Belgian country report, Chapter III.B.6.c.); Section 88 Para. 2 Code of Criminal Procedure (Czech country report, Chapter III.B.6.c.); Articles 100–100-2 Penal Procedure Code (French country report, Chapter III.B.6.b.); Article 588*bis* c. Para. 3 LECRIM (Spanish country report, Chapter III.B.6.c.).

[208] See above-mentioned chapters of respective country reports referring to Section 100e Subsection 3 German StPO; Article 90*quater* Belgian CCP; Section 88 Para. 2 Czech Code of Criminal Procedure; Articles 100–100-2 French Penal Procedure Code; Article 588*bis* c. Para. 3 LECRIM; also see Article 126m Para. 2 Dutch Code of Criminal Procedure; Austrian country report, Chapter III.B.6.a.

[209] See above-mentioned chapters of respective country reports referring to Section 138 Subsection 1 Austrian StPO; Section 34 German StPO; Article 90*quater* Belgian CCP; Section 88 Para. 2 Czech Code of Criminal Procedure; Article 126m Para. 2 Dutch Code of Criminal Procedure; Article 588*bis* c. Para. 3 LECRIM; Austrian country report, Chapter III.B.6.a.

it is carried out in a proportionate manner. To counterbalance the intrusiveness of interference, national legislation in most of the countries requires an interception to be granted only when there exists a certain degree of suspicion and when it is necessary and proportionate. Furthermore, all the countries included in this study limit the possibility of using interception in criminal investigations to certain types of serious crimes. Despite the fact that these safeguards can be found in every national legal order, they can vary from country to country as to checks, balances, and thresholds for authorising interception. This can have an effect on cross-border cooperation in the interception of communications.

a) Predicate offences

All of the countries included in this study limit the availability of the interception of communications as an investigative measure by making it possible only for certain types of offences. While this restriction exists in every national legal order, the approaches to imposing the limitation vary. There are three possible ways to restrict interception to only specific types of crime: by creating a *list of offences* (**Belgium**, **Estonia**, **Germany**, **Poland**, and **Switzerland**), by establishing a *minimum punishment threshold* for crime through the number of years of imprisonment (**Austria**, **France**, and the **United Kingdom**), or by a *combination of both* (**Australia**, **Croatia**, the **Czech Republic**, **Hungary**, **Italy**, the **Netherlands**, and **Sweden**).

– *List of predicate offences*

A list of predicate offences for the purpose of the application of the interception exists in **Belgium**, **Estonia**, **Germany**, **Poland**, and **Switzerland**. In **Germany**, the interception of communications can be granted only in the case of investigations related to certain criminal offences from the list provided in Annex I to the German country report. When interception is considered, this formal requirement is balanced with the need for assessment of the seriousness of the offence in each individual case. In this regard, as pointed out in the German country report, the evaluation of seriousness shall take into account not only the sentencing range but also other considerations, such as the significance of the danger to legally protected interests and other circumstances.[210] Similarly, in **Belgium** and **Estonia**, criminal procedure legislation provides an exclusive list of criminal acts that allow interception to be authorised as a measure in a criminal investigation.[211]

---

[210] German country report, Chapter III.B.7.b.

[211] Belgian country report, Chapter III.B.7.; Estonian country report, Chapter III.C.2.

– *Minimum penalty requirement*

The second approach is taken by **Austria**, **France**, and the **United Kingdom**. However, even while following the model of establishing the minimum penalty requirement, the countries have different regulations in this regard.

In **France**, the law of criminal procedure establishes a minimum penalty threshold for crimes in order to qualify for the application of interception in criminal investigations. According to Article 100 Penal Procedure Code, the interception of correspondence can be used for the investigation of offences if the penalty incurred is equal to or exceeds two years of imprisonment.[212] In **Austria**, interception can be ordered for investigation of intentionally committed offences carrying a minimum prison sentence of more than one year.[213] In the **United Kingdom**, the IPA 2016 restricts the possibility of interception to "serious crimes": the UK Government recently changed the definition of what constitutes a serious crime and lowered the minimum threshold from 3 years or more to 12 months.[214]

– *Combination of list of offences and minimum penalty requirement*

A combination of approaches to limiting interception to certain types of offences by both establishing a minimum penalty threshold and providing for a list of offences can be found in the national procedural legislation of **Australia**, **Croatia**, the **Czech Republic**, **Hungary**, **Italy**, the **Netherlands**, **Portugal**, **Spain**, **Sweden**, and the **United States**.

The **Australian** TIA Act provides that an interception warrant is available for an interception in cases of a serious offence. The definition of "serious offence" covers a broad range of general and specific offences, usually requiring that they be "punishable by imprisonment for life or for a period, or maximum period, of at least 7 years." This threshold is dispensed with regarding some offences, in particular cybercrime-related offences.[215]

The **Croatian** Criminal Procedure Act refers to "all criminal offences punishable by long-term imprisonment" and, in addition, provides a list of predicate offences.[216]

The Code of Criminal Procedure of the **Czech Republic**[217] provides that the interception can be authorised for crimes with a minimum penalty threshold of at least eight years of imprisonment. Furthermore, the following offences are listed, in addition to those meeting the minimum penalty requirement:

---

212 French country report, Chapter III.B.1.

213 Austrian country report, Chapter III.B.7.

214 UK country report, Chapter III.B.7.

215 Australian country report, Chapter III.B.7.

216 Croatian country report, Chapter III.B.7.

217 Para. 1 of Section 88, reference from Czech country report, Chapter III.B.7.b.

- machinations in insolvency proceedings,
- violation of regulations on rules of competition,
- negotiating advantages during public procurement, tender and auction,
- machinations during public procurement and tenders,
- machinations at a public auction,
- misuse of powers of an official person, or
- other intentional criminal offence for which prosecution is stipulated in a declared international treaty.[218]

In **Hungary**, the legislator establishes two penalty thresholds – with the second threshold being lower but subject to an exhaustive list of offences. Firstly, interception can be ordered in relation to intentional crimes punishable by imprisonment of up to five years or more. It may also be used to investigate intentional crimes punishable by imprisonment of up to three years, but the crime needs to be specified in the pertinent exhaustive list.[219]

Portuguese law, in general, stipulates that interception can be ordered for the investigation of criminal offences regarding which a custodial sentence with a maximum limit of over three years applies. In addition, there is a specific list of crimes, which includes a number of offences permitting an application for the interception authorisation.[220]

In **Italy**, according to Article 266, Para. 1 Code of Criminal Procedure, the interception of telephonic or telecommunication conversations or communications is allowed in proceedings against crimes punished with life sentence or imprisonment of more than five years as maximum limit. In addition, the Article contains a list of crimes that can be subject to interception.[221]

Dutch law follows the same approach. Interception can be granted only for the investigation of offences listed in Article 67 Code of Criminal Procedure, which includes crimes allowing for pre-trial detention. This means that, in general, only crimes involving a maximum sentence of more than four years of imprisonment can justify an interception. However, there are certain specifically mentioned offences (Article 67 Para. 1 b), regarding which interception can be granted if a crime involves a less than four-year maximum penalty threshold.[222] For example, most forms of cybercrime are included in the category of specifically mentioned offences.[223] Similarly, the **Swedish** law of criminal procedure – Article 27:18 CJP – es-

---

218 Quoted from Czech country report, Chapter III.B.7.b.

219 Hungarian country report. Chapter III.B.7.

220 Portuguese country report, Chapter III.B.

221 Italian country report, Chapter III.B.7.

222 Dutch country report, Chapter III.B.7.

223 Information obtained during the law enforcement workshop in the Netherlands.

tablishes a minimum penalty requirement of two or more years of imprisonment in order for interception to be granted for the purpose of a preliminary investigation. In addition to offences falling into this category, Para. 2–7 of Section 2 of the same Article provides a list of crimes allowing for interception to be authorised in criminal investigations, even if the minimum penalty does not meet the general requirement.[224]

In **Spain**, the same approach was adopted only few years ago. Up to the enactment of the new legislation in December 2015, interception could be used only in cases of serious crime,[225] meaning crime punished with a minimum of three or more years of imprisonment. However, the new legislation implemented a combination of the minimum penalty requirement and a list of predicate offences. Article 588*ter* a.1 LECRIM establishes that interception can be ordered for an investigation of intentional offences punishable with a term of imprisonment of at least three years and also for offences committed within a group or criminal organisation, as well as for terrorist offences. In addition to these crimes, the law provides that interception of communications can be authorised for the investigation of crimes committed through "computers or IT equipment *(instrumentos informáticos)*, or other information technology, or communication, or communication services."[226]

In the **United States**, the list of offences is combined with a reference to certain crimes. The definition of predicate offences depends on the whether you are dealing with the federal or state level. According to the US report, on the federal level, interception is only available if it may reveal evidence related to a crime that is included in a very detailed list of predicate offences (18 U.S. Code, Section 2516. Authorization for interception of wire, oral, or electronic communications), or the whereabouts of someone fleeing from prosecution regarding one of the aforesaid offenses. On the state level, the application for the interception can be made if it may provide evidence of a felony under state law for murder, drug trafficking, kidnapping, robbery, gambling, child sexual exploitation, child pornography, bribery, extortion, or any other crime dangerous to life, liberty, and property.[227]

b) Degree of suspicion

In addition to limiting the interception of communications to certain types of crimes and dangers, most of the countries establish further safeguards to ensure that the intrusion is balanced. The legal requirement to take into account the degree of

---

[224] Swedish country report, Chapter III.B.6.

[225] Spanish country report, Chapter III.B.7.b. referring to Articles 13 and 33 Criminal Code and Article 579 LECRIM.

[226] Ibid.

[227] USA country report.

suspicion is one such safeguard, and can be found in the legislation of **Australia**, **Croatia**, **Germany**, the **Netherlands**, **Sweden**, and, with some modifications, in **Spain**. The **Czech Republic** follows this principle in practice but without an explicit requirement in the law.

The **Australian** TIA Act requires a certain degree of suspicion for the application for an interception warrant. It demands proof that a person is using or is likely to use a service or device for communication and that information gained in the course of interception will assist the investigation of a serious offence.[228]

The **German** law of criminal procedure establishes the requirement of "an ordinary degree of suspicion of someone having committed or participated in the commission of a serious criminal offence, or in cases where there is criminal liability for attempt, having attempted to commit such an offence or having prepared such an offence by committing a criminal offence."[229] This degree of suspicion, however, is assessed by taking into account the circumstances of the case, which have to provide enough grounds to assume that a person is actually involved in the commission of the crime.[230] In **Belgium**, the court has to assess whether there are serious indications for the commission of a crime.[231] Article 126m of the **Dutch** Code of Criminal Procedure refers to suspicion of a serious criminal offence for which interception is possible and which must be a serious infringement of the legal order.[232] In **Sweden**, Article 27:20 CJP requires reasonable suspicion of an offence for the interception authorisation to be granted.[233]

In two countries – **Spain** and the **Czech Republic** − the degree of suspicion, though not explicitly worded as a necessary prerequisite in the interception provisions, is required in court practice. **Spanish** legislation uses the phrase "sufficient indications of the existence of the criminal offence."[234] The issue of the degree of suspicion has been addressed in Spanish judicial practice in the decisions of the Supreme Court, in particular the Decision of 18 June 1992, which stated that "mere affirmation" and "existence of certain suspicions" do not provide enough justification for authorisation of the interception.[235] Similarly, in the **Czech Republic**, the law of criminal procedure does not expressly include the degree of suspicion requirement. However, this issue is addressed in judicial practice, which stipulates that the degree of suspicion has to be assessed by the court granting interception on

---

228 Australian country report, Chapter III.B.7.

229 Cited from German country report, Chapter III.B.7.a. referring to Section 100a Subsection 1 (1) StPO.

230 German country report, Chapter III.B.7.a.

231 Belgian country report, Chapter III.B.7.a. referring to Article 90*ter* Para. 1 CCP.

232 Dutch country report, Chapter III.B.1., see also Chapter III.B.7. for details.

233 Swedish country report, Chapter III.B.6.

234 Spanish country report, Chapter III.B.7.a.

235 Ibid.

a case-by-case basis. As pointed out in the Czech country report, the Constitutional Court has passed judgements referring to the duty of the judge to evaluate the degree of suspicion and to provide the relevant information in the interception order.[236]

c) Principle of subsidiarity

The principle of subsidiarity represents yet another safeguard explicitly implemented in the legislation of several countries, namely **Australia**, **Belgium**, the **Czech Republic**, **Germany**, **Portugal**, and **Spain**. The application of this principle requires the judge to consider whether other – less intrusive – means of investigation need first to have been tried unsuccessfully or are to be considered unlikely to be successful.

In **Germany**, the law of criminal procedure stipulates that interception can be authorised only when the use of any other less intrusive tools would be much more difficult or of no avail. The degree of difficulty in this regard particularly concerns the application of more time-consuming investigative tools that might significantly delay the investigation itself.[237] Similarly, the **Spanish** country report states that the principle of subsidiarity is provided for in the law and means that the investigating authority and the judge have to assess whether other less intrusive measures could be applied and whether they are likely to be successful.[238] In **Portugal**, it is necessary to prove that the evidence would, by any other means, be impossible or very hard to collect.[239] In **Belgium**, the Code of Criminal Procedure requires the court to evaluate whether other investigative tools may be sufficient. Interception can be granted only if there are reasonable grounds to believe that other methods will not help to "reveal the truth."[240] In this regard, however, the national reporter notes that the parliamentary preparatory works especially highlight that there is no necessity for the court to apply other investigative measures unsuccessfully: the assessment of the judge that other tools will not succeed is sufficient to address the issue of subsidiarity.[241] Similar legal provisions that require an assessment of whether alternative investigation tools could be used and why they would not be successful also exist in **Australia**.[242]

---

236 Czech country report, Chapter III.B.7.a.

237 German country report, Chapter III.B.7.d.

238 Spanish country report, Chapter III.B.7.d.

239 Portuguse country report, Chapter III.B.

240 Belgian country report, Chapter III.B.7.d. referring to Article 90*ter* Para. 1 CCP.

241 Belgian country report, Chapter III.B.7.d. referring to parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communications and telecommunication, Belgian Senate, 1992-1993, 1 September 1993.

242 Australian country report, Chapter III.B.7.

The law of criminal procedure in the **Czech Republic** also refers to the principle of subsidiarity, though in a more general way. According to the national reporter, interception can be authorised only if there are reasonable grounds to believe that it will yield facts relevant to the investigation and that either there is no other way to obtain these facts or that it will significantly reduce the possibility of achieving the aim of investigation.[243] This requirement forces the law enforcement agencies and the court to consider the application of less intrusive measures.[244]

However, not all of the countries follow the approach of establishing subsidiarity requirements. For example, the **French** country report clearly states that the legislation does not establish any obligation to consider or try less intrusive methods of investigation.[245] **Swedish** law does not provide for any specific requirement of reasonable belief that the evidence will be acquired in the course of interception or for consideration of less intrusive measures first, although it does require the measure to be of "particular importance to the investigation."[246] However, as noted in the Swedish report, in practice, the principle of proportionality means that the application of less intrusive investigative measures is at least a factor to consider before the authorisation of interception.[247]

d) Proportionality of interception in individual cases

Another principle that aims to ensure that interception is applied with checks and balances is a specific requirement to address the issue of the proportionality of the measure in each individual case of interception. This requirement exists in the national laws of **Australia**, **Belgium**, **Germany**, **Spain**, and **Sweden**. Even if there is no explicit requirement in the legislation related to interception, the analysis of the national reports shows that a principle of proportionality can be applied in practice, as is done in the **Czech Republic** and **France.**

In **Germany**, the approach to interception follows the concept that such an intrusion must be proportionate in each individual case of investigation.[248] Hence, the application of interception in a criminal investigation contradicts the principle of proportionality if information related to the core area of privacy could possibly be captured in the course of communications acquisition. Another dimension of the principle of proportionality of interception in German legislation is the requirement

---

[243] Czech country report, Chapter III.B.7.d. referring to Section 88 Para. 1 of Act No. 141/1961 Sb., Code of Criminal Procedure.

[244] Czech country report, Chapter III.B.7.d.

[245] French country report, Chapter III.B.6.b.

[246] Swedish country report, Chapter III.B.6.

[247] Ibid.

[248] German country report, Chapter III.B.7.e.

that one must be able to assume that the interception will successfully lead to information related to the particular investigation.[249]

The **Belgian** law of criminal procedure directly obliges the court to assess whether the application of interception in a particular criminal investigation is proportionate to the seriousness of the crime: the investigating judge may authorise interception only if the case is exceptional.[250] A similar requirement can be found in **Swedish** law, which requires interception to be proportionate to the seriousness of the crime in each individual case of criminal investigation: Article 27:21 CJP imposes a duty to specify the conditions aimed at protecting the integrity of the individual whenever interception is considered.[251] The **Spanish** national reporter states that the law requires the judge to assess the proportionality of the measure in each individual case; however, for crimes with a minimum threshold of three years of imprisonment, this requirement is usually considered fulfilled.[252] In **Australia**, the TIA Act requires to assess, in addition to the seriousness of criminal conduct, the extent to which the privacy of a person or persons would be infringed as a result of the interception.[253] The national reports from the **Czech Republic** and **France** highlighted that the legislation in their respective countries does not impose any direct obligations on the authority that grants interception to assess the proportionality of the interception in relation to the seriousness of the crime. In both countries, however, the principle of proportionality is applicable when interception is considered in practice. In the **Czech Republic**, in cases in which law enforcement would apply for too many interception authorisations for one individual case, the court would be very likely to reject the applications pursuant to the "principle of moderation" outlined in Section 2 Para. 4 Code of Criminal Procedure.[254] In **France**, according to the national reporter, requests for interception and justification of the application of such intrusive investigative measures are subject to the general rules on the principle of proportionality in criminal procedure.[255]

e) Persons and connections under surveillance

Almost all country reports indicate that the interception of communications could be directed not only against the accused, but also against other persons not suspected of the offence but whose communications might be of importance for the purpose of the criminal investigation. This principle has to be balanced, however,

---

249 Ibid.

250 Belgian country report, Chapter III.B.7.e. referring to Article 90*ter* Para. 1 CCP.

251 Swedish country report, Chapter III.B.6.

252 Spanish country report, Chapter III.B.7.e.

253 Australian country report, Chapter III.B.7.

254 Czech country report, Chapter III.B.7.e.

255 French country report, Chapters II.A.2 and III.B.7.d.

with certain checks and safeguards to avoid proactive monitoring. Consequently, there are certain regulations at the national level as to what kind of connections can be placed under surveillance in criminal proceedings and which identifiers (names, addresses, or specific connections) can be the subject of the interception order.

In **Germany**, the interception measure can be directed either against a suspect or against other persons if there are certain grounds to believe that they are communicating with the suspect or if the person under investigation might use their devices and connections. The order to intercept must always be issued only in relation to specific persons, though there is no need to know the exact identity of the suspicious persons at the time of interception authorisation. When the identity of the suspect is unknown, the authorisation can provide identifiers, such as a phone number or data allowing for identification of devices or connections, e.g. IP addresses or IMEI. As clarified in the German report, device identification is, however, admissible only when it can be proven that the number has not been assigned to another device at the same time.[256] Similarly, in the **Netherlands** and in the **Czech Republic**, there is no need to know the identity of the suspect. According to **Dutch** legislation, an interception order has to take into account the suspect of the crime, but can be directed against a "user" or numbers.[257] Likewise, in the **Czech Republic**, any user of communication services can be the subject of an interception order as long as all the prerequisites for granting authorisation are fulfilled and the court finds sufficient justification for such interception. As in other countries, the interception order can target a particular number or device, but not specific communication content.[258] In **Sweden**, the order to intercept can be issued only for a particular phone number or other identifiers. The suspect is not the only person against whom interception might be ordered if there are reasonable grounds to believe that the accused will contact a particular number at a particular time.[259]

Croatian law of criminal procedure allows for interception to be ordered, in addition to the suspect, for those persons against whom there are grounds for suspicion that: (1) they have delivered to, or received from the perpetrator of the offences, … information and messages in relation to offences, or (2) the perpetrator has used their telephone or other telecommunications devices, or (3) they have hidden the perpetrator of the criminal offence or helped him.[260] In **Italy**, the law allows interception not only with regard to persons under investigation, but also with regard to other people whose conversations are relevant for the investigation.[261]

---

256 German country report, Chapter III.B.7.c.

257 Dutch country report, Chapter III.B.7.

258 Czech country report, Chapter III.B.7.c.

259 Swedish country report, Chapter III.B.6.

260 Croatian country report, Chapter III.B.7.

261 Italian country report, Chapter III.B.7.

Belgian procedural law, in addition to allowing for the order to be issued against a suspect or persons who are expected to have regular contact with the suspect, explicitly provides for the possibility to direct the warrant to the places where the suspect is expected to stay.[262] **Spanish** legislation also has distinct legal provisions: in addition to the possibility of ordering the interception against a suspect, devices belonging to the suspect, and third parties, the law provides for the possibility to intercept devices that are being used by suspects electronically for illegal purposes without the knowledge of the owner.[263]

In all of the countries, the requirements to specifically identify persons or connections under surveillance serve as safeguards against proactive monitoring. For example, as mentioned in the **Belgian** country report, the issue of proactive monitoring was addressed in the parliamentary preparatory works, which ruled such a measure to be unacceptable and referred to the existence of a suspect as one of the necessary prerequisites for the interception order.[264] However, the report from **Sweden** specifically addressed the question of the employment of interception to target particular content with the use of trigger words. The Swedish national reporter points out that, although this measure is not possible in criminal investigations, it exists for the signals intelligence operations carried out by the National Defence Radio Establishment (FRA) and only in relation to international communications.[265]

f) Consent of a communication participant to the measure

Another divergence in the national legislation comes from the differences in the approaches to interception when one of the parties agrees to the measure. While, as analysed below, there is no need to issue an interception warrant in this case in **Germany**, **Spain**, and – in certain circumstances – in **Australia** and **Austria**, the legislation in **Croatia**, the **Czech Republic**, **Sweden**, and the **United Kingdom** requires a certain authorisation.

– *No authorisation for interception is needed if one communication party consents*

The **German** report clarifies that when one party to the communication exchange permits law enforcement agencies to read or listen to the communication, they do not fall under the scope of the interception provision (Section 100a StPO).

---

[262] Belgian country report, Chapter III.B.7.c. referring to Article 90*ter* §1, 3° CCP.

[263] Spanish country report, Chapter III.B.7.c. referring to Articles 588*bis* h. and 588*ter* c. LECRIM.

[264] Belgian country report, Chapter III.B.7.c. referring to parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1992-1993, 1 September 1993.

[265] Swedish country report, Chapter I.A.3.

The notion behind this is that such interception does not breach the confidentiality of communications: the only breach in this case is that of the trust that one person puts into someone he/she communicates with.[266] In this regard, the interception provision protects the secrecy of communications only against interference by a third party.[267] Similarly, in **Spain**, when consent for the interception is given by one of the communication parties, the interception cannot be considered an unlawful breach of the secrecy of communications, except in cases where an imprisoned person consents to the interception. As the Spanish national reporter points out, the latter requires authorisation in accordance with an European Court of Human Rights judgement.[268]

The **Australian** TIA Act provides a limited number of circumstances when interception is possible with the consent of one party: there need to be reasonable grounds for suspecting that another party to the communication has acted in such a way as to raise suspicion that there might be serious damage such a loss of life, serious personal injury, threat of killing or some other consequences listed in Section 7(4) and (5) TIA Act.[269]

In **Austria**, Section 135 Subsection 2 StPO allows for interception based on consent only in cases involving the consent of the owner of the technical equipment which was or will be the source or destination of the message transmission.[270]

– *Certain authorisation is needed*

In contrast to the approaches requiring no authorisation when one of the parties agrees to interception, several national reports (**Croatia**, the **Czech Republic**, and **Sweden**) indicate that certain authorisation is still needed. However, the approaches to authorisation in this case vary. Stricter regulation exists in **Croatia** and **Sweden**, where an interception order needs to be issued even if one of the parties to the communication has given consent to the interception.[271] As clarified in the **Swedish** country report, this conclusion can be drawn from the judicial practice related to the decisions of the European Court of Human Rights, which requires getting court authorisation to permit the use of hidden microphones in order to record a conversation when a party of the conversation agrees to "wearing a wire."[272] The

---

266 German country report, Chapter III.B.7.f.

267 Ibid.

268 Spanish country report, Chapter III.B.7.f. referring to *M.M. v The Netherlands*, 8 April 2004, No. 39339/98.

269 Australian country report, Chapter III.B.7.

270 Austrian country report, Chapter III.B.7.

271 Croatian country report, Chapter III.B.7.f.; Swedish country report, Chapter III.B.6.

272 Swedish country report Chapter III.B.6.

need for court authorisation in cases of consent for interception is outlined in the documents of the Swedish Commission of Inquiry on Certain Police Methods.[273]

A combination of approaches to authorisation of this particular type of interception is taken in the **Czech Republic**, where a court order is always required, even in cases of consent – except for certain urgent cases (as analysed above in the chapter on urgent warrants), in which case the consent of one party is a necessary prerequisite for the interception of communications with no court authorisation.[274] However, as the national reporter points out, this provision is subject to criticism because, according to the opponents of this measure, it infringes the principle of the secrecy of communications concerning the party who did not consent to interception. As a general rule, this principle is counterbalanced with the requirement for the court to consider whether the intrusion is properly justified. However, in the case of consent, this balance is upset.[275]

While, in the **United Kingdom**, the Investigatory Powers Act (IPA) 2016 stipulates that when one of the parties to the communication has consented to the interception, an interception warrant is not required, this conduct is considered as a form of surveillance and requires authorisation under Part 2 of the Regulation of Investigatory Powers Act 2000 (RIPA 2000). This authorisation differs from the authorisation regime for interception under the IPA 2016.[276]

8. Validity of interception order

a) Maximum length of interception order

The maximum length of the interception order is another issue that highlights differences at the national level and that can affect international cooperation. As revealed by this study, the period of validity of the interception warrants for the purpose of criminal investigation varies from 15 days to 6 months, depending on the national legislation.

The shortest period of validity of the interception warrant is provided in **Italian** criminal procedure: a period of interception cannot exceed 15 days.[277] **Dutch** law limits the maximum length of interception to four weeks.[278] In **Belgium** and **Sweden**, the validity of the interception order cannot exceed one month; in the **United States**, maximum validity is 30 days.[279] **Estonia** establishes two months as a max-

---

273 Ibid.

274 Czech country report, Chapter III.B.7.f.

275 Ibid.

276 UK country report, Chapter III.B.7.

277 Italian country report, Chapter III.B.8.

278 Dutch country report, Chapter III.B.8.

279 USA country report.

imum validity of an interception order.[280] In **Croatia**, **Germany**, **Poland**, **Portugal**, **Spain**, and **Switzerland**,[281] the maximum period of validity is three months, in **Australia**, it is 90 days.[282]

In the **Czech Republic** and **France**, the general period of interception shall not exceed four months. However, **French** legislation provides additional clauses concerning different lengths of interception orders, depending on the purpose of interception and the authority that grants the authorisation. The maximum duration of four months is established in French legislation for the interception of correspondence authorised by the investigating judge and by the judge responsible for enforcing sentences. If the interception of correspondence is ordered by the liberty and custody judge, the duration of the warrant cannot exceed two months in cases of "search for an escaping person" and one month if the case concerns flagrancy or preliminary procedure in relation to a restricted list of penal infringements considered as being organised crime or delinquency." A shorter duration – one month – is provided for in case of a flagrancy investigation or a preliminary investigation in relation to this restricted list. Lastly, correspondence interceptions at the level of terminal equipment ordered by the liberty and custody judge or the investigating judge can have a maximum duration of 48 hours.[283]

The **United Kingdom** has the longest period of validity of interception warrants established in law: six months.[284]

By contrast, no specific maximum duration of the interception order is stipulated in the criminal procedure law of **Austria**. Austrian law of criminal procedure does not set a maximum period of validity of the interception order, stipulating that interception may only be ordered for such a future period of time that is likely to be required in order to fulfil the respective purpose.[285] In **Hungary**, the period of interception has to be specified precisely; however, the national reporter indicates there is no upper limit to the duration of surveillance of communications for specific law enforcement purposes authorised by a judge.[286]

The maximum period of validity of interception orders can in practice be shorter than established by the law. For example, as discussed at the meeting with **Spanish** law enforcement agencies, warrants in Spain, where the maximum duration is three months, in practice are normally issued for no longer than one month, and the po-

---

280 Estonian country report, Chapter III.C.4.

281 See Croatian country report, Chapter III.B.8.; Polish country report, Chapter III.B.8.; Portuguese country report, Chapter III.B.; Switzerland: information obtained at law enforcement workshop.

282 Australian country report, Chapter III.B.8.

283 French country report, Chapter III.B.8.a.

284 UK country report, Chapter III.B.8.

285 Austrian country report, Chapter III.B.8.

286 Hungarian country report, Chapter III.B.8.

lice are obliged to provide the judge with the results of the interception so that he/she can decide whether continued interception is necessary. The same practice exists in Portugal, where the period of validity can be up to three months, but the court normally grants interception for one month only.[287]

b) Prolongation of authorisation

In all of the countries included in this analysis, the interception order can be prolonged for the same period of time, provided the conditions for the interception of communications still exist and interception is still required for the purpose of investigation. The prolongation usually follows the same procedure as the initial application for the interception. Legislation in most of the countries, with some exceptions, establishes neither limits for the number of prolongations nor restrictions for a cumulative period of interception. Such provisions, limiting the time for the cumulative interception of communications, can be found only in some national laws, such as in **Belgian**, **Croatian**, **Estonian**, **French**, **Polish**, and **Spanish** legislation.

In **Belgium**, the Code of Criminal Procedure provides for a maximum prolongation period of six months. As discussed during the workshop with Belgian law enforcement agency representatives, if the interception is still necessary after this period of time, the investigating judge has to start a new interception case and find new circumstances to justify the interception. In **Spain**, which has a maximum three-month period of validity for the interception warrant, the court can extend it for the same period of time, but for no longer than 18 months cumulatively.[288] Similarly, in **Croatia**, after the expiry of the initial three-month period of an interception warrant, the warrant can be extended for another three months, but further extension up to a total of 18 months is possible only for certain serious offences.[289] In **Estonia**, the two-months period for interception can be extended several times, for up to a total of one year; however, after a year, the request for renewal must be made by the prosecutor general.[290] **Polish** criminal procedure law stipulates that there is a possibility to extend the authorisation to intercept in particularly justified cases for a period not exceeding a further three months in addition to the initial three-months period. However, the entire duration may not exceed six months.[291]

French legislation establishes special temporal limits for certain types of interception warrants. There is a limitation on the length of interception of correspondence authorised by the liberty and custody judge: the maximum duration for such

---

287 Information from the law enforcement workshops in Spain and Portugal.

288 Spanish country report, Chapter III.B.8.a.

289 Croatian country report, Chapter III.B.8.

290 Estonian country report, Chapter III.C.4.

291 Polish country report, Chapter III.B.8.

authorisation in case of a misdemeanour is six months, including prolongations. No limit, however, is established for crimes that justify the application of the interception. Further limitations refer to interception warrants issued by the liberty and custody judge with a maximum duration of one month for cases of flagrancy and a number of other infringements. This authorisation to intercept can be renewed only once under the same conditions.[292] A warrant for the use of remote forensic software devices can be issued for a maximum period of four months and prolonged for another four months only under exceptional circumstances (Article 706-102-2 Penal Procedure Code).[293]

It should also be noted that, although the national legislation does not establish limits on the number of possible extensions of interception authorisations in **Sweden**, the country report highlights that the principle of proportionality means that limits are considered in practice when a judge considers authorisation of interception in a particular case. As the national reporter points out, cases such as certain security-related investigations in Sweden in the 1960s, when the warrants were prolonged monthly over a total period of 16 years, would be unacceptable today, even though security operations and organised crime investigations generally last longer.[294]

c) Revocation of authorisation

In most of the countries, there is the possibility of revoking the authorisation; however, the approaches vary concerning the responsibility (duty) to revoke. In **Croatia**, **Germany**, **Spain**, and **Sweden**, the interception order must be revoked under certain circumstances, and revocation is considered a duty of the authority that issued the authorisation. In **Australia**, the duty to revoke lies with the chief of the agency that applied for the warrant.[295]

In contrast, the national reports from **Belgium**, the **Czech Republic**, and **France** indicated that their law establishes no obligation to revoke the interception warrant.

– *Revocation as a duty*

In **Germany**, the law of criminal procedure requires termination of the interception without delay as soon as the prerequisites for authorisation of the measure no longer exist. In this case, both the public prosecutor and the court have the power to revoke the interception order. A revocation is essential in cases in which suspicion is proven to be unfounded, the investigation no longer requires interception, or

---

[292] French country report, Chapter III.B.7.a.

[293] French country report, Chapter III.B.7.b.

[294] Swedish country report, Chapter III.B.7.

[295] Australian country report, Chapter III.B.8.

when it is questionable whether interception will achieve the purpose of the investigation.[296] In **Sweden**, the law obliges the prosecutor or the court to repeal the authorisation immediately if there is no longer any need for the measure.[297] The same approach is followed by **Australia**.[298] According to the **Spanish** national report, national legislation in Spain provides that the interception shall be terminated once the grounds for its authorisation cease to exist or when it becomes clear that the measure will produce no results for the investigation.[299] Similar provisions exist in **Croatia**, where authorisation must be revoked by the investigating judge.[300]

– *No duty to revoke*

In contrast to the approaches where the obligation of the duty to revoke the interception is explicitly stated, the legislation in **Belgium**, the **Czech Republic**, and **France** does not provide for a duty to revoke a warrant. This does not mean, however, that revocation cannot take place. Only the **French** country report indicated that there is no discussion of this issue on the national level, where the law of criminal procedure imposes no obligation to revoke the authorisation of the interception.[301]

In **Belgium** and the **Czech Republic**, despite the absence of a duty to revoke provided for in the law, the revocation may still result from other obligations. Article 90*quinquies* Para. 1 of the **Belgian** Code of Criminal Procedure stipulates that the investigating judge "may" end the interception "as soon as the circumstances that justified the measure have disappeared."[302] As pointed out in the national report, Belgian academic literature argues, however, that the existence of the principle of subsidiarity obliges the judge to revoke the authorisation if interception is no longer necessary.[303] In the **Czech Republic**, the legislation provides no requirements to revoke the authorisation; however, the national report highlights that the revocation might take place when it becomes apparent that there is a lack of substantive grounds for the use of interception. In addition, the report states that, pursuant to Para. 8 of Section 88 Code of Criminal Procedure, the Constitutional Court may also revoke the interception warrant.[304] Furthermore, the police authority in the Czech Republic is required to perform regular checks as to the existence of the reasons that led to the authorisation of interception. If the grounds for authorisation

---

296 German country report, Chapter III.B.8.c.

297 Swedish country report, Chapter III.B.7. referring to Article 27: 23 CJP.

298 Australian country report, Chapter III.B.8.

299 Spanish country report, Chapter III.B.8.c. referring to Article 588*bis* j LECRIM.

300 Croatian country report, Chapter III.B.8.

301 French country report, Chapter III.B.8.a.

302 Belgian country report, Chapter III.B.8.c.

303 Ibid.

304 Czech country report, Chapter III.B.8.c.

have ceased to exist, the police have a duty to terminate the interception without delay, even before the end of the period of the interception order. In this case, the court that gave the authorisation has to be notified in writing.[305]

9. Duties to record, report, and destroy

Additional divergences in the interception procedure can be found in the laws stipulating the duties to produce the interception recording and to report the interception results. Furthermore, there are different approaches to the destruction of the records. These differences will be further analysed in the following part of the study.

a) Duty to record and report

aa) Duty to record interception

Several country reports (**Australia**, the **Czech Republic, France**, **Poland**, and **Spain**) indicated that there is always a duty to produce official records, which is explicitly provided for in the law. Furthermore, in the **Czech Republic** and **Sweden** (where no general duty to record exists), the law imposes a recording duty.

In **Australia**, the TIA Act outlines significant requirements for the recording and reporting of information relevant to interception warrants.[306] In **France**, although the recording procedure varies slightly, depending on the interception regime, there is always a duty to produce official records. For data acquired under the provisions on electronic correspondence interception, Article 100-4 Penal Procedure Code establishes for the official records, which are to be kept under closed official seals, that they should always indicate the time and date of the interception and provide information on the beginning and end of the measure. The same requirement under Article 100-5 Penal Procedure Code exists for any transcriptions of correspondence. In the same manner, in case of remote data capture, an official record is compulsory for each device installed and for each data capture carried out in the course of the investigation. Transcription and description of remote data capture are also the subject of the official records requirement.[307] In **Spain**, the duty to record includes the obligation to submit the information, so that it can be verified as authentic. The recording duty is provided for by Article 588*ter* LECRIM, which requires the police to submit a transcription of the relevant information and the complete recorded data to the judge in a way that will prove its authenticity.[308]

---

[305] Czech country report, Chapter III.B.8.c. referring to Section 88 Para. 3 Code of Criminal Procedure.

[306] Australian country report, Chapter III.B.9.

[307] French country report, Chapter III.B.9.

[308] Spanish country report, Chapter III.B.9.a.

In the **Czech Republic**, in addition to the obligation to record, there is a duty which is linked to the subsequent presentation of the intercepted material in court as evidence. The police investigator is required to evaluate the content acquired during the interception and to prepare the record, which represents a transcript of those data relevant to the investigation. A protocol is mandatory if this record is going to be presented as evidence in court. The Czech Code of Criminal Procedure establishes a set of formal requirements for this protocol: it must "contain information about the place where the interception was conducted, time of interception, manner of the interception, authority which issued the record, and general information about contents of the record."[309] In addition, the protocol must meet another set of formal requirements, which have been established in Section 55 Code of Criminal Procedure for any transcript recordings in criminal proceedings.[310]

Another country with a requirement for recording duties is **Sweden**. The internal Swedish regulation of the Prosecuting Authority, namely Section 7 of the Ordinance on Preliminary Investigation (1947:948), stipulates the obligation of the person leading the investigation to log the interception of communications. These records are, however, not attached to the file of the preliminary investigation: As pointed out in the country report, in practice, the interception is usually only noted in the file in case it might be further used as evidence in criminal proceedings.[311]

In **Belgium**, there is no duty to record; however, the national reporter stated that Article 90*sexies* Code of Criminal Procedure[312] obliges the police officer responsible for the interception in a particular investigation to send the recordings made during the interception to the investigating judge. These recordings must be sent together with the transcripts that the police officer considers relevant for the investigation and any translation thereof. However, this data does not have to be presented as an official record.[313]

bb) Duty to report the progress of interception to judge / prosecutor

There are different approaches to the duty to report the progress of interception. In several countries, namely **Croatia**, the **Czech Republic**, **Germany**, **Estonia**, and **Sweden**, the law imposes no special obligation to report on interception progress during the process of application of the measure. The absence of this duty, however, can still be balanced with additional checks during or after the interception. In **Germany**, there is a requirement to notify the court that granted the author-

---

309 Czech country report, Chapter III.B.9.a. referring to Section 88 Para. 6 Code of Criminal Procedure.

310 Czech country report, Chapter III.B.9.a.

311 Swedish country report, Chapter III.B.8.

312 Article 90*sexies* CCP, translation from Belgian report, Chapter III.B.9.a.

313 Belgian country report, Chapter III.B.9.a. referring to Article 90*septies* Para. 1 CCP.

isation to intercept about the results of the interception.[314] The **Croatian** Code of Penal Procedure imposes an obligation on the police to draw up daily reports about the application of the interception order and document technical recordings. These recordings must be delivered to the State Attorney upon request.[315] In the **Czech Republic**, as a balancing measure, the record of the interception must be made available to the public prosecutor who is, in turn, obliged to perform regular checks concerning the legality of the interception and its progress.[316] In **Sweden**, as stated by the national reporter, the absence of a reporting duty is balanced with the short validity period of the interception warrant, which means that the prosecutor is required to report to the court the circumstances of the interception once the application for the extension has been made.[317]

In contrast, there are formal obligations to report to the court on the progress of interception in **Belgium** and **France**. In **Belgium**, the police are required to submit reports to an investigating judge about the course of interception every five days.[318] As pointed out during the practical workshop with Belgian law enforcement agency representatives, the report usually includes technical details, information about the intercepted person, and details about the progress of the interception. Furthermore, the judge has to be informed by the police in cases in which the phone number or other identification has changed. Similarly, in **France**, the police have to report to the investigating judge about the progress of the measures related to the interception of communications.[319] Different reporting regulations can be found in the **Netherlands**, where the police do not have to inform the court on the progress of interception;[320] however, there is an obligation to report to the prosecutor who issued the interception requisition.[321]

In **Spain**, although there is no direct legal obligation on the frequency of providing information on the progress of interception, the comprehensive judicial oversight in criminal investigations entails reporting duties in practice.[322] As shared by Spanish law enforcement agency representatives during the workshop, the judge or the prosecutor can request information on the performance of the interception every week, every 15 days, and at the end of the validity period of the interception war-

---

314 German country report, Chapter III.B.9.a. referring to Section 100e Subsection 5 Sentence 2 StPO.

315 Croatian country report, Chapter III.B.9.

316 Czech country report, Chapter III.B.9.a.

317 Swedish country report, Chapter III.B.8.

318 Belgian country report, Chapter III.B.9.a. referring to Article 90*quater* Para. 3, 2° CCP.

319 French country report, Chapter III.B.9.

320 Dutch country report, Chapter III.B.9.

321 Information obtained at the law enforcement workshop in the Netherlands.

322 Spanish country report, Chapter III.B.9.a.

rant. Upon such request, the police have to provide the transcripts and all other information about the interception progress.

b) Duty to destroy

Another safeguard concerning the interception of communications is the duty to destroy the records, and is provided for by the national law in almost all the jurisdictions covered by this study. The grounds for such destruction and the bodies responsible for it vary from country to country.

In **France**, **Germany**, the **Netherlands**, **Poland**, and **Sweden**, the decision on record destruction belongs to the prosecutor. **French** legislation leaves the decision on the destruction of records to the public prosecutor; however, Article 100-6 of the French Penal Procedure Code stipulates that the reason for record destruction is "expiry of the limitation period for prosecution."[323] **German** legislation requires deletion without delay of the personal data acquired during the course of the interception if they are no longer deemed necessary for the purpose of the investigation and are not the subject of a court review of the investigative measure.[324] Both technical recordings and written material are to be destroyed; furthermore, the deletion must be officially documented. When the data represent accidental discoveries that are not related to the main proceedings but can be used as evidence in other criminal proceedings, the requirement to delete is not applicable. The public prosecutor takes into consideration all decisions on deletion of data; however, if the case is pending, it is the court that decides whether the intercepted data shall be destroyed.[325] In the **Netherlands**, the information collected by means of interception must be destroyed two months after the intercepted person was notified about the interception. However, the prosecutor in control of the interception can postpone the destruction if the data is needed in another investigation or if data have to be stored in the serious crime register. The destruction must be officially documented in the records.[326] The **Polish** Code of Criminal Procedure stipulates that if the records contain information that has no relevance to the criminal proceedings, the public prosecutor shall submit a motion after interception has ended, requiring that all recordings be destroyed. The decision on this motion shall be made by a court without delay, in a hearing without participation of the parties.[327] **Swedish** legislation provides for the responsibility of the public prosecutor to order the destruction of all records having no relevance to the aim of the interception authorisation and which will not be used as evidence in criminal proceedings. As pointed out in the

---

[323] French country report, Chapter III.B.9.

[324] German country report, Chapter III.B.9.b. referring to Section 101 Subsection 8 StPO.

[325] Ibid.

[326] Dutch country report, Chapter III.B.9.

[327] Polish country report, Chapter III.B.9.

national report, the Swedish Commission on Security and Integrity Protection has criticised both the police and prosecutors for significant delays in carrying out the duty to destroy the records of interception and, as a result of these checks, the Chief Public Prosecutor's Office adopted new guidelines in 2012, specifically addressing this issue.[328] A different approach to the distribution of responsibility to destroy data can be found in **Australia**, where the obligation to arrange the destruction of records falls on the chief officer of a law enforcement agency.[329]

In **Belgium**, it is also the police authorities that are named as the bodies responsible for carrying out the duty to destroy. A police officer responsible for implementation of the interception has to destroy any information that is not kept in an official record.[330] The destruction must also be officially recorded.[331] In **Spain** and in the **Czech Republic**, it is also the duty of the police to destroy the records; however, the law provides for the necessary time period between conclusion of the investigation and destruction. According to the law of criminal procedure in the Czech Republic, the destruction shall take place three years after final conclusion of the case and only with the consent of the public prosecutor.[332] In Spain, a provision on the duty to destroy makes a distinction between original records and preserved copies of the interception data. While the original records are to be destroyed upon court order after the final ruling on termination of criminal proceedings, the preserved copies have to be kept for five years after the penalty was executed or when the time for the prosecution has expired or when the acquittal decision becomes final.[333]

10. Notification duties and remedies

a) Duty to notify persons affected by the measure

– *Legislation on the duty to notify*

As one of the safeguards, some of the countries demand notification about the interception. Such a requirement can be found in the legislation in **Austria**, **Belgium**, **Estonia**, **Germany**, **Italy**, the **Netherlands**, **Spain**, and **Sweden**.[334] A different

---

328 Swedish country report, Chapter III.B.8. referring to ÅM RättsPM 2012:8.

329 Australian country report, Chapter III.B.9.

330 Belgian country report, Chapter III.B.9.b. referring to Article 90*septies* Para. 1 CCP.

331 Ibid.

332 Czech country report, Chapter III.B.9.b. referring to Para. 7 of Section 88 Code of Criminal Procedure.

333 Spanish country report, Chapter III.B.9.b. referring to Article 588*bis* k LECRIM.

334 Austrian country report, Chapter III.B.10.; Dutch country report, Chapter III.B.10.; German country report, Chapter III.B.10.a. referring to Section 101 Subsection 4 StPO; Czech country report, Chapter III.B.10.a. referring to Sections 88(8) and 88(9) Code of Criminal Procedure; Spanish country report, Chapter III.B.10.a. Article 588*ter* i.3

approach is taken in countries like **France**, which has legislation stipulating the duty to notify affected persons after the interception has ended. In France, due to the concept of the secrecy of the interception measures, it is only the accused that can learn about the interception and only after he/she is given access to the case files.[335]

– *Exemptions from the duty to notify*

While stipulating the obligation to notify affected parties, the **Czech Republic**, **Estonia**, **Germany**, the **Netherlands**, and **Sweden** provide in their laws for exceptions from this duty when certain conditions are met. These conditions, as shown below, vary depending on the jurisdiction.

In the **Czech Republic**, the obligation to inform the suspect constitutes an administrative procedure; the duty of notification is not applicable in cases of certain crimes, or when a criminal investigation is being carried out against several persons and has not yet been completed in relation to at least one of them, or when such notification can pose threats to "national security, life, health, or the rights and freedoms of individuals, etc."[336]

In **Estonia**, an exemption from the duty to notify is granted when such notification may significantly endanger the criminal proceedings, damage the rights and freedoms of another person which are guaranteed by law, or endanger another person. Further exceptions refer to jeopardising confidentiality of the methods and tactics of a surveillance agency or the equipment or police agent used in conducting surveillance activities, and confidentiality of an undercover agent or a person who has been recruited for secret cooperation. The permission for the exemption can only be given by the prosecutor's office.[337]

In **Germany**, the duty to notify can be waived in cases in which such notification can damage the protected interests of such persons, e.g. damaging the interests or reputation of the accused after no incriminating evidence has been found or when the person is not significantly affected by the measure and there are reasons to believe that there is no interest in such notification. The latter exception is, therefore, applicable only to those targets that were not a primary subject of the interception.[338] Such notification is to be carried out as soon as possible, unless it poses a threat to the aim of the criminal investigation or "the life, physical integrity and

---

LECRIM; Swedish country report, Chapter III.B.9.; Italian country report, Chapter III.B.10.; Estonian country report, Chapter III.C.7.

335 French country report, Chapter III.B.10.

336 Czech country report, Chapter III.B.10.a. referring to Section 88 Para. 9 Code of Criminal Procedure.

337 Estonian country report, Chapter III.C.7.

338 German country report.

personal liberty of another person, or significant assets."[339] In cases in which notification was postponed for more than 12 months on the above-mentioned grounds, there is a requirement of court approval for any further delays. In cases in which it can be foreseen that the reasons for the delay will not cease to exist, a court has the power to authorise the permanent dispensation of the notification about interception.[340]

Similarly, **Dutch** legislation makes exceptions from the rule of notification in cases in which the person has already been granted access to the criminal investigation file or if notification is not reasonably possible. These reasons might include the impossibility of finding out the identity or address of the person or situations when disclosure of the wiretapping constitutes a security risk.[341]

Swedish legislation provides for an exemption from the notification requirement in cases in which it is obviously unnecessary, when such notification can be detrimental to an ongoing investigation, in certain cases of mutual legal assistance, or when notification can be harmful to the personal or economic integrity of an individual. Other exceptions from the notification duty are provided for offences within the jurisdiction of the security police. In such investigations, notification can be postponed until the secrecy rules are no longer applicable; however, one year after the investigation is complete, the duty to notify expires, even if notification has not been made. As pointed out in the Swedish national report, notification for these types of investigations is very unlikely; all cases of non-notification are under the supervision of the Commission on Security and Integrity Protection.[342]

b) Remedies

Five of eighteen countries included in this study provide for remedies which intercepted persons can use against the measure. The set of remedies ranges from judicial reviews (in **Belgium**, the **Czech Republic**, and **Germany**), to complaints and damage claims in civil procedures (in **Spain** and **Sweden**).

Two countries – the **Czech Republic** and **Germany** – provide for an interception-related specific remedy as an opportunity to initiate judicial review for cases of interception. In the **Czech Republic**, Section 88 Para. 8 Code of Criminal Procedure stipulates that a person whose communications have been intercepted can apply to the Supreme Court in order to challenge the lawfulness of the authorisation for interception. The procedure for such judicial review is regulated under the gen-

---

[339] German country report, Chapter III.B.10.a. referring to Section 101 Subsection 5 StPO.

[340] Ibid.

[341] Information obtained at the law enforcement workshop, see also Dutch country report, Chapter III.B.10.

[342] Swedish country report, Chapter III.B.9.

eral provisions 314l–314n Code of Criminal Procedure.[343] In **Germany**, Section 101 Subsection 7 StPO allows, through a judicial review, any person who has been the subject of communication interception to challenge the legality of the measure and the way it was carried out. The application must be filed two weeks after the notification of interception has been received.[344] Another country in which judicial review is generally possible is **Belgium**. However, as pointed out in the national report, there is no specific remedy stipulated specifically for cases of interception. The affected person can file a complaint against the performed measure under the general rules provided by the Code of Criminal Procedure to challenge the legality of investigative measures.[345]

In **Sweden**, despite the fact that a person affected by interception theoretically has several possibilities to challenge the measure – either to file a complaint with the Commission on Security and Integrity Protection, or to appeal against the measure to the chief government law officer (the Chancellor of Justice), or to use a civil court procedure to claim damages –, the national reporter states that no such cases are known to have occurred since the 1980s.[346] **Spanish** legislation also has several possible remedies for a third person affected by interception, such as initiating a criminal accusation of unlawful infringement or claiming damages in civil proceedings. However, since the duty to notify third parties was introduced together with new legislation and had not yet entered into force at the time of writing of the Spanish national report, the reporter points out that no practical analysis can be made regarding this issue.[347]

c) Criminal consequences of unlawful interception measures

In all of the countries included in this study, illegal interception constitutes a criminal offence. However, the national reports from **Germany** and **Spain** especially highlighted that unlawful interception carried out by law enforcement will entail these particular consequences. **German** criminal law prohibits unlawful eavesdropping or recording of non-publicly spoken words under Section 201 StGB, which stipulates higher sentences for public officials. If the interception of communications does not meet the requirements established by the German law of criminal procedure, it entails criminal liability if knowledge and intent for such a crime exist. Furthermore, some cases of unlawful interception in information systems might theoretically fall under provisions dealing with illegal access (Section 202a

343 Czech country report, Chapter III.B.10.b.

344 German country report, Chapter III.B.10.b.

345 Belgian country report, Chapter III.B.10.b.

346 Swedish country report, Chapter III.B.9.

347 Spanish country report, Chapter III.B.10.b.

StGB) and illegal interception (Section 202b StGB).[348] The **Spanish** report states that an official involved in unlawful interception would face disciplinary sanctions with the possibility of dismissal,[349] in addition to criminal liability for interference with the secrecy of communications.

In the **Czech Republic**, there is also a general provision on violation of the confidentiality of messages, which stipulates criminal responsibility for unlawful interception (Section 182 Penal Code). In addition, as stated in the national report, if a judge authorises interception illegally, criminal liability might also follow pursuant to the prohibition on the abuse of powers of an official person (Section 329 Penal Code).[350] Similarly, the **Swedish** report highlights that unlawful surveillance operations can entail criminal responsibility for the misuse of office. In this case, the overseeing body – the Commission on Security and Integrity Protection – has to report this offence for further prosecution.[351]

In **Belgium**, the criminal offence of unlawful interception is covered by Articles 314*bis* and 259*bis* Criminal Code. The Belgian national reporter states that, since data on the breach of law concerning the interception of communications is not available, it is impossible to provide information on specific sanctions for infringement of the rules on the investigating procedure. However, as noted in the report, a violation of the duty to notify those who were intercepted about the interception might entail disciplinary or civil sanctions.[352]

The **French** report highlights that, in addition to the criminal responsibility that might be faced for unlawful interception, there are also consequences for the validity of the evidence in cases where certain requirements outlined in the criminal procedure legislation for the interception are not met. These consequences do not, however, include criminal responsibility and refer mostly to the penalty of nullity, e.g. in the case of interception of privileged communications without following the special procedure of notification of respective chambers and professional associations.[353]

11. Confidentiality requirements

a) Obligations of telecommunication service providers to maintain secrecy

Legislation in most of the countries included in this analysis requires communications service providers to maintain secrecy about the interception of commu-

---

348 German country report, Chapter III.B.10.c.

349 Spanish country report, Chapter III.B.10.c.

350 Czech country report, Chapter III.B.10.c.

351 Swedish country report, Chapter III.B.9.

352 Belgian country report, Chapter III.B.10.c.

353 French country report, Chapter III.B.9.

nications. On the national level, this is achieved by the implementation of special provisions to maintain the confidentiality of the interception in either a telecommunication regulation, as in **Australia**, **Germany**, and **Sweden**,[354] or in criminal or criminal procedural law, as in **Belgium**, **Hungary**, and **Spain**.[355] Furthermore, this obligation can fall under the general provisions on the duty to cooperate, as found in the **Czech Republic** and **France**,[356] using a mixed approach: the obligation to maintain secrecy of communications is secured by the virtue of both special legislation and a general prohibition on disclosure.[357]

b) Sanctions against telecommunications service providers and their employees

In most of the countries, a violation of the duty to maintain secrecy entails criminal liability, although the thresholds for sanctions might vary. **Australia**, the **Czech Republic**, **Germany**, and **Sweden** outline criminal responsibility in their special regulations on telecommunications, while **Belgium**, **France**, and **Spain** provide for criminal sanctions in the criminal code or the law on criminal procedure.

In **Australia**, a violation of the obligation of secrecy is punishable by imprisonment not exceeding two years. In addition, recently introduced legislation on technical assistance requirements provides that unlawful disclosure of information is an offence punishable by imprisonment for up to five years.[358] In the **Czech Republic**, violation of the duty of secrecy can be punished either under specific legislation (Article 118 Act on Electronic Communications), with a fine of up to 20,000,000 CZK, or under the general provisions on disclosure of classified information, as an administrative offence with a fine of up to 5,000,000 CZK. Furthermore, Sections 317 or 318 Code of Criminal Procedure establish criminal liability for endangering classified information, providing for different imprisonment terms depending on the gravity of the offence.[359] In **Germany**, a violation of the obligation to maintain secrecy constitutes a regulatory offence punishable with a fine of up to

---

354 Australian country report, Chapter III.B.11. referring to Section 276 (1) Telecommunications Act; German country report, Chapter III.B.11.a. referring to Section 5 Subsection 4 Sections 1 and 15 TKÜV; Swedish country report, Chapter III.B.10. referring to Section 6:20-23 Act on Electronic Communications.

355 Belgian country report, Chapter III.B.11.a. referring Article 90*quater* Para. 2 and 4 Code of Criminal Procedure; Spanish country report, Chapter III.B.11.a. referring to Article 588*ter* e LECRIM; Hungarian country report referring to Section 265 Para. (3) Criminal Code.

356 French country report, Chapter III.B.11. referring to Articles 226-13 and 226-14 Penal Procedure Code.

357 According to the Czech country report, Chapter III.B.11., the special obligation is provided for in Section 97 Para. 8 Act on Electronic Communications. In addition, Act No. 412/2005 Sb. prohibits the unauthorised disclosure of classified information and is thus applicable to the obligation to maintain secrecy.

358 Australian country report, Chapter III.B.11.

359 Czech country report, Chapter III.B.11.

500,000 EUR (Section 149 Subsection 1 (22), Subsection 2 (1) TKG). Furthermore, disclosure of interception entails a punishment of up to two years of imprisonment or a fine (Section 18 G 10 Act).[360] **Swedish** legislation on electronic communications (ECA 7:15) also refers to criminal sanctions provided by the criminal code and by legislation on the breach of secrecy (in the Act on Transparency and Secrecy).[361]

Belgium, **France**, **Hungary**, **Italy**, and **Spain** provide for criminal responsibility for breach of the obligation to maintain secrecy. In **Belgium**, the violation of secrecy obligations is punished in accordance with Article 458 Penal Code.[362] The **Hungarian** country report indicates that the employees of electronic communication service providers participating in secret information gathering shall be punishable with imprisonment of two to eight years in accordance with the Section 265 Criminal Code for the crime of "abuse of classified data" if they breach their obligation of confidentiality.[363] In **Spain**, Article 588*ter* e LECRIM provides for criminal liability for disobeying a judicial order when persons fail to fulfil the duties outlined in the provisions on the duty to cooperate, including the obligation to maintain secrecy.[364] **French** legislation also provides for penal sanctions in accordance with Articles 226-13 and 226-14 Penal Procedure Code.[365] According to the **Italian** country reporters, disclosure of the information that a person is under surveillance or disclosure of the content of the interceptions is punishable as a crime pursuant to Article 326 Criminal Code.[366]

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

a) Collection of traffic data

aa) Relevant information

The importance nowadays of metadata in criminal investigations can hardly be overestimated. During the practical workshops in every country included in this study, the law enforcement representatives stated that content data and metadata are equally important for the purpose of investigation. Often, the law enforcement

---

360 German country report, Chapter III.B.11.b.

361 Swedish country report, Chapter III.B.10.

362 Belgian country report, Chapter III.B.11.b.

363 Hungarian country report, Chapter III.B.11.

364 Spanish country report, Chapter III.B.11.b.

365 French country report, Chapter III.B.11.

366 Italian country report, Chapter III.B.11.

agencies have to examine both content and traffic/subscriber data or investigate one type of data before requesting another category of information, e.g. analysis of metadata can precede the interception of communications. The importance of the interception of metadata (not access to stored data) is also increasing because the investigation can benefit from information about communication if the content is encrypted.

All the countries included in this study have either general or specific legal provisions for traffic data requests. The following regulations have been indicated in the national reports:

- **Australia**: Telecommunications (Interception and Access) Act 1979 (general provisions on disclosure of information or documents)
- **Austria**: Section 134 (2) StPO
- **Belgium**: Article 88*bis* Code of Criminal Procedure
- **Croatia**: Article 339.a Criminal Procedure Act
- **Czech Republic**: Article 88a Code of Criminal Procedure
- **Estonia**: Section 90[1] Code of Criminal Procedure
- **France**: Articles 77-1-1 (preliminary investigation), 60-1 (flagrancy) and 99-3 (investigating judge) Penal Procedure Code
- **Germany**: Section 100g StPO
- **Hungary**: E-Communications Act
- **Italy**: Article 132 decreto legislativo 196/2003
- **Netherlands**: Article 126n Code of Criminal Procedure
- **Poland**: Article 218 Para. 1 Code of Criminal Procedure
- **Portugal**: Law 32/2008, Cybercrime Law, Penal Procedure Code
- **Spain**: Article 588*ter* j. LECRIM
- **Sweden**: Section 19 CJP
- **Switzerland**: Article 273 Code of Criminal Procedure
- **United Kingdom**: IPA 2016, Part 3

bb) Substantive prerequisites of collection

Substantive prerequisites for orders concerning traffic data vary in the national legislations. Most of the countries – namely **Australia**, **Austria**, **Belgium**, **Croatia**, the **Czech Republic**, **Germany**, the **Netherlands**, **Portugal**, **Spain**, **Sweden**, and the **United Kingdom** – permit the application of this measure only in relation to specific crimes or require a certain degree of suspicion. By contrast, countries such as **Estonia**, **France**, **Hungary**, **Italy**, and **Poland** do not provide for such safeguards. The analysis of these requirements is provided below on the basis of distinguishing between these two approaches.

– *Specific crimes and/or degree of suspicion as prerequisites*

Austrian law permits collection of traffic data in case of kidnapping. Furthermore, traffic data can be collected for investigation of intentional offences that carry a minimum prison term of more than six months if the owner of the technical equipment, which was or will be the source or the target of a message transmission, expressly agrees to it. Without owner's permission, traffic data can be obtained in case of intentional offences that carry a minimum prison term of more than one year.[367]

German law establishes two substantive prerequisites, one regarding the nature of the offence committed, and the other regarding the degree of suspicion concerning the targeted person. Section 100g StPO provides that there must be certain grounds to believe that the person whose traffic data are to be collected has been involved in the commission of the offence, either as a perpetrator or as a participant.[368] In addition, the offence itself must have either substantial significance,[369] or have been committed via telecommunication means.[370] The question of significance is assessed in accordance with court practice, which considers the element of "substantial significance" to be a decisive factor for the infringement of a person's rights.[371] A recent judgement of the German Federal Constitutional Court provides that offences with a maximum penalty threshold of five-year imprisonment do not always exhibit the element of substantial significance, and thus justification of the intrusion into civil rights has to be decided based on the circumstances of the individual case. Misdemeanours with a maximum punishment of less than two years of imprisonment cannot be considered offences of substantial significance. For offences committed via telecommunication means, the subsidiarity principle must always be taken into consideration.[372] Similarly, **Swiss** law – Article 273 Code of Criminal Procedure – requires a strong suspicion of a felony or misdemeanour for collection of traffic data.[373]

Some countries provide for a minimum penalty threshold as a prerequisite for traffic data collection. In the **Czech Republic**, the minimum penalty threshold established in the legislation – Section 88a Code of Criminal Procedure – provides that traffic data collection can be ordered only for crimes with a penalty threshold of a minimum of three years of imprisonment, with the exception of crimes that

---

367 Austrian country report, Chapter III.C.2.

368 German country report, Chapter III.C.1.a.

369 German country report, Chapter III.C.1.a. referring to Section 100g Subsection 1 Section 1 No. 1 StPO.

370 German country report, Chapter III.C.1.a. referring to Section 100g Subsection 1 Sesction 2 No. 2 StPO.

371 German country report, Chapter III.C.1.a.

372 Ibid.

373 Information obtained at the law enforcement workshop.

cannot be investigated without such data, e.g. crimes committed using electronic communications.[374] Furthermore, as in the case of substantive prerequisites for interception, traffic data can be obtained in the investigation of an intentional crime which the Czech Republic must prosecute by virtue of an international treaty. Ultimately, the substantive prerequisite is the application of the principle of subsidiarity.[375]

Similarly, in **Australia** and **Spain**, the penalty threshold is written in the law. In **Australia**, for data that do not exist yet and will be generated in the future an authorisation for collection has a higher threshold than authorisation for obtaining historical information or documents. Collection of traffic data of communication that will happen in the future can be authorised only in case of there being suspicion of a serious offence or an offence against a law of the Commonwealth, a State, or a Territory that is punishable by imprisonment for at least three years.[376] According to the **Spanish** report, the substantive requirements are the same as those for the interception of communications. Although there have been debates in Spanish academic literature that intrusion in the case of traffic data collection is less severe than in the case of interception, and the requirements should therefore have a lower threshold, Spanish law still requires the same degree of suspicion for both measures and limits both of them to offences with a minimum penalty higher than three years of imprisonment, organised crime or terrorism, and cybercrime.[377] Furthermore, the law requires the data to be indispensable for the investigation.[378] The same approach concerning offences justifying the collection of traffic data can be found in the **Netherlands**, where, despite the fact that the collection of traffic data does not require judicial approval, it can be applied only to investigations of the same categories of crimes as those for interception.[379] **Swedish** legislation provides that traffic data collection may be ordered for offences with a penalty of at least six months of imprisonment or for some other categories of offences, e.g. hacking, drug trafficking, etc.[380] In **Belgium**, the law provides for a minimum penalty requirement – one year of imprisonment –and outlines the requirements for proportionality and

---

[374] Czech country report, Chapter III.C.1.a. referring to the section of the Penal Code No. 40/2009 Sb., which includes the following list of offences: violating the secrecy of conveyed messages (Section 182), fraud (Section 209), unlawfully gained access to a computer system or data carrier (Section 230), acquisition and receipt of access, equipment, or codes for computer systems or other similar data (Section 231), criminal threat (Section 353), stalking (Section 354), spreading of false news (Section 357), incitement (Section 364), and criminal connivance (Section 365).

[375] Czech country report, Chapter III.C.1.a.

[376] Australian country report, Chapter III.C.1.

[377] Spanish country report, Chapter III.C.1.a.

[378] Ibid., referring to Article 588*ter* j LECRIM.

[379] Dutch country report, Chapter III.C.1. referring to Articles 126n and 67 Code of Criminal Procedure.

[380] Swedish country report, Chapter III.C.1.

subsidiarity.[381] **Croatian** law stipulates that traffic data can be collected for the offences that could justify the interception of content, as well as all other offences punishable by imprisonment of at least five years or more.[382] In the **United Kingdom**, traffic data can be collected only in relation to investigations of serious crimes.[383]

– *No requirement concerning degree of suspicion or specific crimes*

France has only general provisions allowing for the collection of traffic data without establishing specific requirements concerning the degree of suspicion or specific crimes. The French Penal Procedure Code does not establish specific requirements concerning the degree of suspicion and does not limit requests for traffic data to particular types of crime or a minimum penalty requirement.[384] **Estonian** legislation on criminal procedure stipulates that requests for traffic data can be made only if this is unavoidably necessary for the achievement of the objectives of criminal proceedings.[385] In **Hungary**, traffic data can be requested by the investigating authority, the public prosecutor, the court, or the national security service when authorised by law, provided it is necessary to carry out their respective duties.[386] In **Italy**, traffic data can be requested for any criminal proceedings, for any type of criminal offence, even a minor one. No minimum standard of suspicion is required concerning the person under investigation. Traffic data collection is always possible, at the sole condition that a criminal proceeding be taking place.[387] In the **Polish** law of criminal procedure, the main prerequisite for requesting traffic data is their relevance for an ongoing criminal proceeding (at the investigation or trial phase). The threshold for requesting the data is suspicion of an offence.[388]

cc) Formal prerequisites of collection

National laws differ concerning the need for judicial approval for the collection of traffic data. In **France**, **Italy**, the **Netherlands**, and **Poland**, court authorisation is not required: the public prosecutor or judicial police officer can make a request for the collection of traffic data on their own, without the court approval.[389] In **Aus-**

---

381 Belgian country report, Chapter III.C.1.a. referring to Article 88*bis* CPP and the Data Retention Act of 29 May 2016.

382 Croatian country report, Chapter III.C.1.

383 UK country report, Chapter III.C.1.

384 French country report, Chapter III.C.1.a.

385 Estonian country report, Chapter III.C.

386 Hungarian country report, Chapter III.C.1.

387 Italian country report, Chapter III.C.1

388 Polish country report, Chapter III.C.1.

389 French country report, Chapter III.C.1.a.; Dutch country report, Chapter III.C.1.; Polish country report, Chapter III.C.1.; Italian country report, Chapter III.C.1.

tralia, in addition to disclosure requests that can be submitted by enforcement agencies without court authorisation, the law allows a service provider to voluntarily disclose information or a document to an enforcement agency if it is reasonably necessary for the enforcement of the criminal law. This type of disclosure envisages situations where a service provider becomes aware of the information in the course of business.[390]

By contrast, in **Austria**, the **Czech Republic**, **Germany**, **Portugal**, and **Spain**, legislation provides that the request for traffic data collection requires judicial approval.[391] The same requirement exists in **Sweden**; however, according to the national report, there are some exceptions to this rule. Although the collection of traffic data in preliminary investigations requires court authorisation, both the police and the security police may order this measure without judicial authorisation as a part of intelligence work under the Act on the Collection of Data on Electronic Communications in Law Enforcement Intelligence (2012:278) if the request can be made on the reasonable suspicion of involvement in a "criminal activity."[392] **Belgium** has a mixed model concerning judicial authorisation: while the request for traffic data is made by the investigating judge under normal circumstances, a public prosecutor is also empowered to give such an order in case of *flagrante delicto* for specific offences listed in Article 90*ter* Para. 2, 3 and 4 Code of Criminal Procedure. However, such an order has to be confirmed by the investigating judge within 24 hours. Judicial confirmation is not required for the offences of taking hostages or extortion by force.[393]

dd) Duty of addressees to disclose information

All of the country reports state that communications providers must supply the necessary information upon receiving an order for traffic data collection. Furthermore, some of the national reporters additionally give the penalties applicable to those providers who refuse to cooperate. For example, such refusal is punishable in **France** by one year of imprisonment and a fine of 75,000 EUR.[394] The **Swedish** report notes that administrative fines are also applicable.[395]

Two of the reports point to the practical problems of compliance with the orders for traffic data collection. The **Czech** report mentions that, in practice, orders for

---

390 Australian country report, Chapter III.C.1.

391 Czech, German, and Spanish country reports, Chapters III.C.1.a.; Austrian country report, Chapter III.C.2.; Portuguese country report, Chapter III.A.

392 Swedish country report, Chapter III.C.1.

393 Belgian country report, Chapter III.C.1.a.

394 French country report, Chapter III.C.1.b. referring to Article 6, VI of law n°2004-575 of 21 June 2004 regarding confidence in the digital economy.

395 Swedish country report, Chapter III.C.1.

traffic data are carefully evaluated on the part of service providers and, if the request is not specific enough or does not contain all the information required by legislation, the provider might refuse to provide the data.[396] Furthermore, the **Swedish** report also notes that, after the EU Court of Justice had declared the data retention directive null and void, some of the service providers in Sweden refused to comply with requests from law enforcement agencies concerning traffic data handovers for those procedures where requests had not been authorised by the court. Since the Swedish telecommunications regulator (PTS) was unsure of whether such procedures were in compliance with the judgement of the European Court of Justice, the duty to cooperate in these cases was not enforced before the PTS came to the conclusion that the legislation contains enough safeguards for such procedures. After this decision of the PTS, enforcement was resumed; however, two of the intermediaries appealed: at the time of writing of the Swedish report, one of them was still not cooperating and was thus facing the possibility of an administrative fine.[397]

ee) Automated procedure of disclosure

Most of the country reports either state that an automatic procedure does not exist (the **Belgian**, **Czech**, **German**, and **Swedish** reports) or provide no information concerning the current arrangements regarding automatic data transfers. The **Swedish** report further notes that the security police had attempted to introduce such procedures several times but faced resistance from the communication providers because the Swedish market is highly competitive and the operators consider a high level of data integrity a competitive advantage that can be advertised in order to attract customers.[398]

b) Collection of subscriber data

aa) Relevant information

The collection of subscriber data is regulated in the national jurisdictions in the following provisions:

- **Australia**: Telecommunications (Interception and Access) Act 1979 (general provisions on disclosure of information or documents)
- **Austria**: Section 76a StPO, Section 92 Subsection 3 (3) TKG 2003
- **Belgium**: Article 46*bis* Code of Criminal Procedure
- **Croatia**: Article 263 Criminal Procedure Act
- **Czech Republic**: Sections 88a and 8 Code of Criminal Procedure

---

396 Czech country report, Chapter III.C.1.a.

397 Swedish country report, Chapter III.C.2.

398 Ibid.

- **Estonia**: Section 90[1] Code of Criminal Procedure
- **France**: Article L. 33-1, V Post and Electronic Communications Code, Articles 77-1-1 (preliminary investigation), 60-1 (flagrancy) and 99-3 (investigating judge) Penal Procedure Code
- **Germany**: Section 100j StPO
- **Hungary**: E-Communications Act
- **Italy**: Article 132 decreto legislativo 196/2003
- **Poland**: Article 218 Para. 1 Code of Criminal Procedure
- **Portugal**: Article 14 Law on Cybercrime
- **Spain**: Articles 588*ter* m and 588*ter* k LECRIM
- **Sweden**: Electronic Communications Act
- **Switzerland**: Article 273 Code of Criminal Procedure
- **United Kingdom**: IPA 2016, Part 3

bb) Prerequisites of data collection

In most of the countries, court approval is not required for orders concerning the provision of subscriber data. In certain jurisdictions, however, such as in the **Czech Republic**, **Germany**, and **Spain**, this rule has some exceptions.

National reporters from **Austria**, **Belgium, Croatia**, **France, Italy**, **Portugal**, **Sweden**, and **the United Kingdom** indicate that no judicial approval is needed. In **Austria**, the request for subscriber data can be made by the criminal police, public prosecutors, and courts; this request does not have to be substantiated.[399] In **Belgium**, the request must be authorised by the public prosecutor;[400] in **France,** the order can be issued either by the prosecutor or by a judicial police officer.[401] In **Sweden**, as stated in the country report, the request for subscriber information is not considered a serious intrusion into personal integrity, so no requirements concerning specific offences have been introduced into Swedish law. Access to subscriber information shall be provided to the law enforcement each time it is necessary for the criminal investigation.[402]

In other states, the requirement of court approval depends on different circumstances, such as the nature of the data or the type of communications provider. In **German** law, Article 100j StPO, in contrast to the collection of traffic data, does not specify special requirements for subscriber data orders regarding the degree of

---

[399] Austrian country report, Chapter III.C.1.

[400] Belgian country report, Chapter III.C.1.b. referring to Articles 46*bis* Para. 2 CCP, 46*bis* Para. 1, 3° CCP.

[401] French country report, Chapter III.C.1.a.

[402] Swedish country report, Chapter III.C.1.

suspicion or a particular type of offence. In general, the provision of data can be ordered without court authorisation upon a request made by the public prosecutor, except when such a request is directed at information concerning access control codes. In the latter case, information may only be requested if the statutory requirements for the use of such data have been met, with the consequence that, in some cases, prior court authorisation is required or other prerequisites must be fulfilled.[403]

The **Czech** report further mentions that the necessity for court approval depends on the type of provider that is requested to supply subscriber data. For orders directed to the providers of IP application-level services, there is no need for judicial authorisation unless the data fall under the obligation of secrecy.[404] For requests to providers at the IP transport level, court authorisation is a necessary prerequisite, and the law stipulates the application of the same substantive and formal requirements as for the collection of traffic data.[405]

In **Spain**, in accordance with Article 588*ter* m LECRIM, the public prosecutor or judicial police are allowed to request subscriber data related to the telephone or other communication service directly from the company providing such service. However, in accordance with Article 588*ter* k LECRIM, in cases concerning offences committed via the internet, court authorisation is required when the judicial officers have access to an IP that is being used to commit a crime and neither can the equipment or identity of the user be identified, nor can the equipment be located.[406]

cc) Duty of addressees to disclose information in manual and automated procedures

All of the national reports indicate that their national legislation provides for the duty to cooperate in case of an order to disclose subscriber data. Concerning the possibility of an automatic procedure, some of the country reporters note that the application of such a technique is possible. For example, in **Germany**, Section 113 TKG stipulates a manual procedure for the transfer of such data; however, automatic data transfers are possible in some cases in accordance with Section 112 TKG concerning the data mentioned in Section 111 Subsection 1 Sentence 1, 3, 4 and Subsection 2 TKG.[407] In such an automatic procedure, the data can be accessed by the Federal Network Agency, which hands them over to the requesting body.[408] The **Belgian** report states that the automatic procedure was installed "for electronic

---

403 German country report, Chapter III.C.1.b.

404 Czech country report, Chapter III.C.1.b.

405 Ibid.

406 Spanish country report, Chapter III.C.1.b.

407 German country report, Chapter III.C.1.b.cc.

408 Ibid.

communications networks that were granted numbering capacity" by Article 3 Para. 2 of the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communication.[409] This automatic procedure involves access via a secure application over the internet. The application sends the request to the communications operator who must then process the request and address it immediately. The **Spanish** report also noted that subscriber data are provided automatically.[410] In contrast, the **Czech** and **Swedish** country reports explicitly stated that there is no automatic procedure.

c) "Data retention"

While Directive 2006/24/EG on data retention (requiring EU Member States to implement the provisions obliging providers to retain certain communication data) was declared invalid by the ECJ in 2014, all of the countries included in this study adopted the provisions on data retention. Concerning the period for such retention, however, the rules vary. The shortest data retention period can be found in **Germany** – recently, approved legislation makes providers retain data for ten weeks (four weeks for location data). In the **Czech Republic**, **Sweden**, and **Switzerland**, the data retention period is six months. In **Portugal**, the data must be retained for six months or one year, depending on the type of data. Other countries, such as **Belgium**, **Poland**, **Spain**, and the **United Kingdom** have longer retention periods – 12 months. **Croatia**, **Estonia**, and **France** establish one year as the term for retaining data. The longest data retention periods can be found in Australian and Italian laws: two years in **Australia** and 72 months (six years) in **Italy**.[411] The **German** and **Czech** country reports indicate controversies at the national level concerning the legislation on data retention. This includes challenging the respective laws in court and refinements of the legislation. The **German** legislation on data retention was first introduced in 2007 by Section 113a TKG in an effort to implement Directive 2006/24/EG. This provision was later declared unconstitutional by the judgement of the Federal Constitutional Court of 02.03.2010.[412] However, in October 2015, the German Parliament voted for a new law, which introduced revised data retention rules. Pursuant to the new law, the time period for data retention has been reduced from six months to ten weeks, with four weeks for location data. Furthermore, the law limits the scope of the data that are to be retained, as well as the cases in which law enforcement can use such data.[413] This law has not been en-

---

[409] Belgian country report, Chapter III.C.1.b. referring to Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications, Belgian Official Journal, 10 February 2003.

[410] Spanish country report, Chapter III.C.1.b.

[411] Australian country report, Chapter III.C.1.; Italian country report, Chapter III.C.1.

[412] German country report, Chapter III.C.1.c.

[413] Ibid.

forced yet, because the Higher Administrative Court of Münster found that, in particular, the German provision permitting unoccasioned data retention, Section 113b TKG, did not define the required objective criteria suited to establish a link between the data and the objective pursued and, thus, did not limit the groups of persons concerned.[414] As a result of the Münster Higher Administrative Court's decision, the Federal Network Agency decided not to enforce the obligation under Section 113b TKG until further notice. Telecommunications providers are therefore still permitted to retain data, but do not have to fear any consequences if they do not comply.[415]

The **Czech Republic** also encountered problems when legislating data retention. The first law was introduced on the 1 May 2005 by the Act on Electronic Communications, which was amended by Act No. 247/2008, following the adoption of the EU Directive 2006. Even after the amendments, the legislation went far beyond the requirements of the Directive in its scope and was challenged in the Constitutional Court, which declared the legislation unconstitutional. The revised data retention legislation was passed in 2012 by Act No. 273/2012 Sb., which introduced stricter rules for data retention.[416]

The problem with data retention in the aftermath of the decision of the EU Court of Justice in 2014 was highlighted in the **Dutch** report: the ECJ ruling led to a Dutch court declaring the Dutch Data Retention Act invalid. A new Data Retention Bill was introduced later to replace the framework on data retention, but the timeline for the approval of the Bill is still unclear at the time this report is being written.[417]

2. Identification of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

a) Identification of device ID with the help of IMSI catchers

Some of the country reports addressed the issue of the use of procedural law in their respective countries for the identification of device ID (IMEI), card numbers (IMSI), and the location of mobile terminal devices. Most of the national reporters in this case, however, state that, when/if such measures are used, they either fall under the general provisions on traffic data or geo-location or are not regulated at all.

Two countries indicate in the reports that specific provisions exist in their national laws, with **Germany** being the only country where such data acquisition represents a specially designed measure: it is provided for in Section 100i StPO and

---

[414] German country report referring to BeckOK-StPO/*Bär*, 34th edition, 1 July 2019, Section 113 TKG recital 10 et seq.

[415] Ibid.

[416] Czech country report, Chapter III.C.1.c.

[417] Dutch country report, Chapter III.C.1.

limited to IMSI catchers.[418] In **France**, Articles 706-95-4 and 706-95-5 PPC provide the investigating judge and the liberty and custody judge with the power to authorise, for the purpose of the repression of organised crime, the capture of technical connection data through the use of a "technical device," which primarily refers to a "proximity technical device" (IMSI catcher).[419] Furthermore, in **Switzerland**, during the law enforcement workshop, the participants shared that the Swiss legislation covers IMSI catchers, which are used for interception by the police.

No specific provisions exist in other jurisdictions. In **Belgium**, there is no legislation concerning the identification of IMEI and IMSI; however, the academic literature considers such measures possible in accordance with Article 46*bis* Code of Criminal Procedure concerning access to identification data.[420] In **Spain**, there is also no legal provision explicitly covering the use of such tools, although, according to the national reporter, they are applied by the law enforcement agencies.[421] Furthermore, in Spain, the judicial practice of the Supreme Court stipulated that, since such measures are used to track the presence of mobile devices in certain locations and thus do not affect personal data, court authorisation is not necessary.[422] The use of IMSI catchers is not regulated in **Sweden**; however, they are utilised in practice, although rarely, according to the Swedish report. The **Czech** report states that such measures are not provided for in the national legislation.

b) Location determination via "silent SMS"

The use of "silent SMS," which are not visible to the owner of the mobile phone, to determine location is also possible under the current legislation in some countries included in this study: this possibility is indicated in the **Belgian**, **French**, **German**, and **Spanish** country reports. Such SMS can play a significant role, both in intelligence and in criminal investigation. For example, according to **German** statistics, "in the first half of 2018 alone, the Federal Office for the Protection of the Constitution, the Federal Criminal Police Office, and the Federal Police sent a combined 173,202 'silent SMS'."[423]

Despite the use of this tool, according to the **German** country report, the legal basis for such a measure is still under discussion. In this regard, the main issue for a long debate in Germany was whether Sections 100a et seq. StPO in conjunction with Sections 163 Subsection 1, 161 Subsection 1 StPO are applicable to the active

---

418 German country report, Chapter III.C.2.a.

419 French country report, Chapter III.C.2.

420 Belgian report, Chapter III.C.2.a. referring to *Kerkhofs/Van Linthout*, Cybercrime, Politeia, Brussels, 2013, p. 356.

421 Spanish country report, Chapter III.C.2.a.

422 Ibid.

423 German country report, Chapter III.C.2.b.

generation of data.[424] This debate ended with a ruling of the German Federal Court of Justice (BGH) in its decision of 8 February 2018 – 3 StR 400/17, in which it declared that such measures may be based on Section 100i Subsection 1 (2) StPO.[425]

In **Belgium**, the use of silent SMS has been approved by the Ministry of Justice as one of the measures falling under the scope of the provisions of Article 88*bis* Code of Criminal Procedure on tracing traffic data and localisation.[426] In **Spain**, the possibility to use this tool is not explicitly provided for in the current legislation; however, according to the Spanish reporter, the police use silent SMS in criminal investigations.[427] The **Czech** report notes that silent SMS are not dealt with in Czech legislation.[428]

D. Access to (Temporarily) Stored Communication Data

1. Online searches with the help of remote forensic software

Legislation permitting the use of remote forensic software is both a source of divergences in the national laws and a very heated issue in the current discussion on investigative powers. In recent years, a number of countries enacted legal provisions allowing law enforcement to use this type of software. As was briefly discussed in Chapter III.B.4.b. of this study, several countries included into this analysis – **Australia**, **Austria**, **France**, and **Spain** – explicitly permit and regulate the use of remote forensic tools, with some of them, like Austria, the Netherlands, or the United Kingdom having adopted this legislation relatively recently. For example, in Austria, the provision on the use of such an investigative tool is not applicable at the time of drafting this report, as the new legislation does not enter into force until 1 April 2020.

All other national reports highlight that there is a lack of powers concerning such an investigative measure in the law of criminal procedure and that remote forensic software is an issue of current debate. In **Croatia** and the **Czech Republic**, the use of remote forensic software has not been clearly addressed in the law of criminal procedure, which raises the question as to whether the use of special tools for remote data capture is permissible. In **Sweden**, the use of remote surveillance is possible, but it requires physical installation and cannot be planted into a computer system remotely. These problems are now discussed in detail.

---

424 Ibid

425 German country report referring to BGH NStZ 2018, 611, 613.

426 Belgian country report, Chapter III.C.2.b.

427 Spanish country report, Chapter III.C.2.b.

428 Czech country report, Chapter III.C.2.

– *The use of remote forensic software is explicitly permitted*

Several countries out of the eighteen jurisdictions included in this study, namely **Australia**, **Austria**, **France**, **Germany**, the **Netherlands**, **Spain**, **Switzerland** and the **United Kingdom**, have special legal provisions explicitly regulating the use of remote forensic software. In some of the countries, however, these measures are considered to be separate powers related to the interception of communications rather than accompanying investigative powers.[429]

In **Australia**, a new Computer Access Warrant regime was introduced in 2018 to allow law enforcement to access data held on computers, including mobile phones. An agency can apply for this type of warrant to investigate an offence punishable by a maximum term of imprisonment of three years or more or a life sentence. The warrant has restrictions for "adding, coping, deleting or altering other data."[430]

In **Germany**, after much debate, the legislator in August 2017 introduced Section 100b StPO, which contains a provision permitting "online-searches" for the purpose of criminal prosecution. For the application of the measure, it is necessary that certain facts give rise to the suspicion that a person, either as perpetrator or participant, has committed a particularly serious criminal offence or has attempted to commit such an offence, that the offence constitutes one of particular gravity in the individual case and that other means of establishing the facts or the whereabouts of the person accused would be much more difficult or offer no prospect of success. The measure may generally only be ordered against the person accused of the crime. Only if, on the basis of certain facts, it can be assumed that the accused him- or herself uses the targeted computer system and that the intrusion into the systems of the accused will not suffice for establishing the facts or the whereabouts, may "online-searches" also be ordered against third parties. Furthermore, the legislator introduced separate legal provisions governing the so-called source telecommunication surveillance. Section 100a Subsection 1 StPO now explicitly provides that "[t]elecommunications may also be intercepted and recorded in such a manner that technical means are used to interfere with the information technology systems used by the person concerned if this is necessary to enable interception and recording in unencrypted form in particular." In addition, the reformed provision allows for the interception of the "content and the circumstances of the communication stored in the person concerned's information technology systems" even after the communication is concluded, provided that this information "could also have been intercepted and recorded in encrypted form during ongoing transmission processes."[431]

---

[429] See, e.g. French country report Chapter III.; Spanish country report, Chapter III.

[430] Australian country report, Chapter III.D.1., referring to Section 27E *Surveillance Devices Act 2005.*

[431] German country report, Chapter III.B.2.c.aa.

Most of the countries explicitly limit the application of remote forensic software to serious crime and require stricter approval procedures compared to interception. In **France**, the power of law enforcement to use remote forensic is provided for in Article 706-102-1 Penal Procedure Code, which permits the judge, after consultation with the prosecutor, to authorise a police officer to set up a technical device, without consent of the person affected, in order to remotely access computer data and record, retain, and transmit them. This concerns data from the input or data recorded and transmitted by audio-visual services. These operations should be performed under the control of the judge and can be used only for the investigation of serious offences.[432]

Similarly, in **Austria**, the application of the measure is very restricted: it can be used only in case of very specific crimes outlined in an exhaustive list (such as, e.g. crimes carrying a prison term of more than ten years or crimes committed within criminal or terrorist organisations). The measure requires court authorisation based on a reasoned order by the public prosecutor. Surveillance of encrypted messages is only admissible if the forensic software is removed or deleted after the investigation has ended. The computer system on which the forensic software is installed and other computer systems must not be damaged in the course of the investigative measure.[433]

In the **Netherlands**, Article 126nba Code of Criminal Procedure allows for penetration of a computer system that is used by a suspect – if necessary, by technical means. This can be done only in case of investigation of a crime that allows for pre-trial detention (Article 67 Sub. 1 Code of Criminal Procedure), only if the act – in view of its nature or its connection with other crimes committed by the suspect – constitutes a serious infringement of the rule of law, and only if the investigation urgently requires the use of the measure. If the above-mentioned substantive prerequisites are met and a criminal act is being investigated for which a maximum prison sentence of at least eight years applies, the remote forensic software can also be used to investigate the recording of data stored on the computer system or of data that will be stored during the period of validity of the order, to the extent reasonably necessary to bring the truth to light, or to render data inaccessible. The requirements for approval are very strict: for the authorisation to use remote forensic software, the investigative officer must send an application to the public prosecutor, who in turn will have to receive prior authorisation from a Central Review Committee and the Attorney General's Office. Only then can the application be approved by the court.[434]

---

[432] Information obtained during law enforcement workshop: serious offences in this regard are the crimes listed in Article 706-73 Penal Procedure Code (such as organised crime, drug trafficking, kidnapping, etc.).

[433] Austrian country report, Chapter III.D.1.

[434] Dutch country report, Chapter III.D.1.

In **Italy**, it is possible to use remote forensic software *(captatore informatico)* for audio surveillance via installation of the remote forensic software on an electronic device. Such use is allowed only in case of ongoing criminal activity related to particular serious crimes listed in Article 51 Para. 3*bis* and 3*quater* Code of Criminal Procedure (i.e., organised crime and terrorism). The use of remote forensic software must be authorised by the judge or a prosecutor in case of urgency with further approval of the court. The judge authorising the use of the measure (and the prosecutor, in case of urgency) must justify this decision and provide reasons for the choice of the tool. Only programs respecting technical parameters identified by the Minister of Justice by decree can be installed on electronic devices for interceptions.[435]

In **Switzerland**, as was discussed during the respective law enforcement workshop, there exists the possibility to use the remote interception software for communications surveillance, as outlined in the new Article 269*quater* Code of Criminal Procedure. The catalogue of crimes for such a measure is more restrictive and the application for authorisation requires subsidiarity: the need to prove that other surveillance measures have not or will not be successful. However, while the application of the measure is restricted, the procedure for authorisation is the same as in the case of interception, with the prosecutor initiating the use of software and a subsequent court authorisation: the court approval should follow the installation of the software.

By contrast, the use of remote forensic software in **Spain** has a broader scope, because it covers not only serious crimes, but also crimes committed with the use of computer tools. The use of remote forensic software was introduced into Spanish criminal procedural law quite recently by the new Law 13/2015 of 5 October 2015 (LECRIM). In accordance with Article 588*septies* a LECRIM, the court can give permission to "use identification data and codes, as well as the installation of a software that allow the electronic remote search, without knowledge of the owner or user, of the contents of a computer, and electronic device, a computer system, or instruments for mass storage of computer data, or databases"[436] in investigations concerning offences committed by criminal organisations, terrorist crimes, crimes committed by means of computer tools or other information technology or telecommunications or a communications service, and a number of other serious offences exhaustively listed in the same provision.[437]

---

435 Italian country report, Chapters III.B.2 and D.1

436 Spanish country report, Chapter III.D.1.

437 Ibid.

– *The use of remote forensic software is not explicitly regulated in the law*

According to the **Hungarian** country report, there is no explicit provision in Hungarian law that allows for the use of remote forensic software; however, the Criminal Procedure Act refers to such coercive measure as "search" *(kutatás)*, which can be applied not only to houses, but also to vehicles and information technology systems. This search can be used if it leads to the finding of an asset that can or has to be confiscated or for the search of an information technology system or data carrier. Data stored on such devices can be considered evidence.[438]

In **Portugal**, there is no explicit provision allowing for the use of remote forensic software; however, Article 19 of the Cybercrime Law is applicable. The law enforcement agencies consider the use of remote forensic software to intercept communication as permissible as long as it is used only for interception and not for hampering or modifying a computer system or a device.[439]

Similarly, the opinion that the use of remote tools might be legally possible under the above-mentioned Section 158 Code of Criminal Procedure was voiced by the **Czech** law enforcement representatives at the workshop, despite the fact that there are no accompanying investigative measures provided for in Czech procedural law concerning the interception of communications. Furthermore, as stated in the Czech country report, the law enforcement agencies can access private places in a clandestine manner under Section 82 Code of Criminal Procedure[440] or acquire knowledge of persons and items in a classified manner by technical or other means under Section 158d of the Code.[441] However, the representatives at the law enforcement workshop stated that they did not know whether remote forensic software had ever been used in the Czech Republic.

– *Physical installation of remote forensic software is required*

Even if the use of remote surveillance techniques is currently allowed under general criminal procedural provisions, like those in Belgium and Sweden, the law enforcement agencies may face practical challenges because of the absence of rules allowing remote installation of such software. In **Belgium** (Article 90*ter* Para. 2 Code of Criminal Procedure), legislation allows clandestine access to private places, e.g. houses, for the purpose of installing equipment to carry out the interception of communications as an accompanying measure. However, as the national reporter points out, in Belgium, the parliamentary preparatory works outline the strict prohibition on intrusion into a computer system (hacking) for performance of an inter-

---

438 Hungarian country report, Chapter III.D.1.

439 Portuguese country report, Chapter III.C.

440 Czech country report, Chapter III.D.1.

441 Ibid.

ception in accordance with Article 90*ter* Code of Criminal Procedure.[442] This requirement makes remote surveillance problematic in many cases.

Law enforcement agencies in **Sweden** face the same practical problems. The Swedish report notes that, while it is possible to get permission from the court to break into private places to install the interception equipment, and this provision possibly covers such tools as key loggers, the fact that such access entails costs and comes with technical problems makes such cases very rare.[443] The national reporter indicated that the current debate concerning additional powers to use remote forensic software is being initiated by the Swedish Security Police, which argues that the law empowers agencies to use these techniques. This conclusion was supported by the Commission of Inquiry, which suggested implementing such tools.[444]

2. Search and seizure of stored communication data

a) Provisions on search and seizure

Approaches to the search and seizure of stored data differ at the national level concerning the existence of special provisions covering such investigative measures. While some of the states, like **Spain** and **Belgium**, have implemented specific frameworks for such measures, general rules on search and seizure are applicable to electronic data in other jurisdictions, as is the case in **Croatia**, the **Czech Republic**, **France**, **Hungary**, **Poland**, and **Sweden**. Some countries, like **Germany** and the **Netherlands**, use both general and specific provisions, depending on the individual case.

– *Both general and special provisions are applicable*

In **Germany**, Section 94 StPO provides for the seizure of objects, which also includes electronic data. Furthermore, Section 110 StPO features a special provision in Para. 3 on the examination of an electronic storage medium, permitting the examination of such a medium on the premises of the person affected by the search to be extended to also cover physically separate storage media insofar as they are accessible from the storage medium. In addition, according to the German country report, the general provisions of Sections 102 and 103 StPO also cover the search of computers and other devices.[445] Similarly, in the **Netherlands**, according to the information obtained during the law enforcement workshop, in addition to the ap-

---

[442] Belgian country report, Chapter III.B.4.b. referring to parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1992-1993, 1 September 1993.

[443] Swedish country report, Chapter III.B.3.

[444] Ibid.

[445] German country report, Chapter III.D.2.

plication of a special provision regulating the seizure of (and access to) stored electronic data – Part 2 of Article 126ng Code of Criminal Procedure – law enforcement agencies can use search and seizure in accordance with general provisions. The Dutch country report also highlights the application of Article 125i Code of Criminal Procedure, which allows for the search of a place to secure data that is stored or fixed on a data carrier in that location. The definition of data is broad enough to cover a computer, external data storage such as a USB stick, and even paper.[446]

– *General provision applies to search and seizure of data*

The **French**, **Hungarian**, and **Polish** reports stated that there are no special provisions on the search and seizure of electronic data; thus, general provisions cover such measures, with the same safeguards being applicable.[447] In the **Czech Republic**, the law provides no special regulation concerning the search and seizure of stored communication data. Therefore, the general provisions are also applicable. According to the Czech report, the data itself cannot be seized, so the police have to acquire the storage media under the provision on property seizure or the provisions on house and personal searches.[448] The **Croatian** national reporters point out that the Criminal Procedure Act stipulates in Article 257(1) that the search of movable property extends to (1) computers, (2) devices connected to the computer, (3) other devices for collecting, saving and transfer of data; telephone, computer, and other communications, and (4) data carriers (mediums). In several decisions, the Croatian Supreme Court has upheld the practice of searching various electronic devices based on Article 275 CPA.[449] According to the **Swedish** report, application of the general provisions on search and seizure is only possible as an open measure and only for data delivered to the recipient and stored on his/her device. For any data in possession of the service providers, a warrant for the interception is required.[450]

– *Special provisions*

Some countries, like **Belgium** and **Spain**, have developed special provisions that cover as many aspects of the search as possible. The **Belgian** Code of Criminal Procedure contains three articles related to network search: Articles 39*bis* (non-secret network search during data seizure), Article 89*ter* (network search during looking-in operations), and Article 90*ter* (secret interception and secret network

---

446 Dutch country report, Chapter III.D.2.

447 French country report, Chapter III.D.1.; Polish country report, Chapter III.D.2.; Hungarian country report, Chapter III.D.2.

448 Czech country report, Chapter III.D.2.

449 Croatian country report, Chapter III.D.2

450 Swedish country report, Chapter III.D.

search). The latter also empowers Belgian law enforcement to access data in the cloud.[451] The new **Spanish** legislation 13/2005 of 5 October 2015 introduced a special regulation on the search and seizure of electronic data. Articles 588*sexies* a–c LECRIM – cover all possible aspects of such a search and seizure, from establishing the requirements for judicial authorisation to the process of making copies of relevant information.[452]

b–c) Access to communications in transmission and access to stored communications

One of the most important questions concerning the interception of communications is the possible difference in the protection of communication in transmission versus stored data. In the modern-day world, the transmission of communication can take a few seconds and then the data is stored on the servers of the provider or on the user's device. However, in some countries, the safeguards for access to stored data are lower than those for the protection of communications in transmission. This situation raises significant concerns with regard to how access to stored communication is treated in the national laws of criminal procedure. In practice, this issue is solved in different ways at the national level. In **Australia**, **Germany**, and **France**, the search and seizure provisions are applicable to such situations. Some of the countries, such as **Spain**, provide the same safeguards for stored and transmitted communications, thus solving this problem. Others, like the **Czech Republic** and **Sweden,** require an interception warrant or a combination of warrants.

– *Seizure provisions are applicable*

In **Germany**, the question of which legal basis may be used to obtain e-mails that are stored on the communication provider's server shows the blurring of the lines between communications in transmission and stored communications. According to the country report, a recent decision of the Constitutional Court has clarified that, within the context of a search and seizure of the suspect's premises, investigators can request the provider to grant a copy of an e-mail account under the normal seizure provision (Section 94 StPO) without judicial authorisation. A former decision by the Federal Court of Justice had determined that if such a production order is executed without the suspect's knowledge, the request could be made with a judicial warrant under the provision admitting the seizure of postal items (Section 99 StPO). This would also include future communication. Nevertheless, according to the country report, after the aforementioned decision of the Constitutional Court, the academic literature argues that a request for stored communication content without the suspect's knowledge can only be made under the same condi-

[451] Belgian country report, Chapter III.D.1.

[452] Spanish country report, Chapter III.D.2.a.

tions as the interception of telecommunications (Section 100a StPO). This means that a judicial warrant is needed and that the investigation must be related to a specific qualified criminal offence listed in Section 100a Subsection 2 StPO.[453]

In **France**, although the safeguards for search and seizure are lower than those provided for the interception of communications,[454] seizure in practice is an applicable measure. As shared by the French law enforcement agency representatives during the workshop, there are several approaches to obtaining access to e-mails stored in electronic mailboxes. When e-mails are stored on the server of the provider, the police can use a production order[455] to obtain the content of stored communications. If the data and e-mails are not stored on the servers of a communications provider – e.g. when the suspect uses a program that downloads e-mails and deletes them from the server – one possible option is search and seizure.[456]

– *The same safeguards are established for both types of communications*

In the **Netherlands**, according to the Dutch law enforcement representatives, the safeguards for interception and access to stored communications are the same; thus, it is not easier to obtain access to the content of a communication after transmission has ended. Access to the stored content is provided for by Article 126ng Part 2 Code of Criminal Procedure and has the same requirements and safeguards as the interception of communications, thus requiring authorisation by a judge. Similarly, according to the **Spanish** country report, the new legislation in Spain provides for the same safeguards for both communications in transmission and stored communications. The only issue that might arise in this regard, as the national reporter notes, is the lack of clarity of the new legislation, which does not distinguish between ordinary files and stored communications.[457]

However, even with the stricter safeguards, the problem of the level of protection can still remain. The **Dutch** report points out that while law enforcement personnel have to use Article 126ng Code of Criminal Procedure, which stipulates that an authorisation by an investigative judge is compulsory, for the access to e-mail messages stored by a communications provider, retrieving similar data from a provider that is not considered to be such a communications provider (e.g. some cloud services) falls under the provision on production orders in Article 126nd Code of Criminal Procedure, which does not require court authorisation.[458]

---

453 German country report, Chapter III.D.2.d.

454 French country report, Chapter III.B.2.

455 Articles 60-1, 77-1-1, 99-3 Penal Procedure Code.

456 Article 56 Penal Procedure Code.

457 Spanish country report, Chapter III.D.2.b.

458 Dutch country report. Chapter II.B.2.

Interception warrant or combination of warrants is necessary to access certain types of stored communications

The practice of accessing certain stored communications with either an interception warrant or a combination of warrants, as gleaned from analysis of the country reports and information from the law enforcement workshops in the **Czech Republic** and **Sweden**, results from disputes over the differences between stored communications and communications in transmission and the lack of legal safeguards for the latter. Each country, however, solves this situation in a different way.

The **Czech** country report states that stored data and communications in transmission have different levels of protection, with the latter enjoying a higher degree of applicable safeguards.[459] The Code of Criminal Procedure, according to the national reporter, is too old to be able to address the issue of blurred borders between stored communications and those in transmission.[460] At the law enforcement workshop, the Czech representatives stated that, because of the high degree of fragmentation of the approaches to accessing stored e-mail content, this issue was addressed in the special recommendations of the Supreme Public Prosecutor's Office for the purpose of unifying legal practice. The application of the legal provisions recommended by this document depends on the nature of the communications that are to be seized or intercepted. When content had been localised on a seized data carrier before the time of its seizure, an interception order is not necessary. For communications that may arrive after seizure of the medium, the use of the seizure order or – as carried out in practice – the order to obtain traffic data is not sufficient. For such acquisitions of data in mailboxes, the Supreme Public Prosecutor's Office recommends applying for court authorisation of surveillance of persons and items according to Section 158d (1), (3) Code of Criminal Procedure.[461]

In **Sweden**, provisions regulating seizure are applicable only to data delivered to the recipient and stored on his/her own device. The interception warrant, according to the national reporter, is required for any data stored on the servers of the providers.[462] Swedish law enforcement representatives at the national workshop confirmed this approach. According to them, this model of authorisation was developed as the result of a long discussion in Sweden on how to prove whether an e-mail has already reached the recipient, and it was intended to solve the problem of read/unread e-mails. Interestingly, the Swedish approach to search and seizure and interception differs, depending on whether a communications provider is a regulated entity or not. Whereas an interception order is always needed for communi-

---

459 Czech country report, Chapter II.B.2.b.

460 Ibid.

461 Supreme Public Prosecutor's Office, 1 SL 760/2014, Collection of Explanatory Opinions of the Supreme Public Prosecutor's Office, Brno, January 26, 2015, File No. 1/2015. Czech representatives provided the document after the law enforcement workshop.

462 Swedish country report, Chapter III.D.

cations stored on the servers of regulated providers, law enforcement agencies can use a search and seizure warrant for access to data stored by information society service intermediaries, because these providers are not considered communication services. Furthermore, Swedish law enforcement representatives noted that, in order to avoid any controversies, the seized device should immediately be disconnected from all networks, so that no new communication can arrive. It should be noted that the requirements for search and seizure in Sweden are also lower than for interception: according to the Swedish representatives, in the case of search and seizure, there is no need for a court order. The requirement for search and seizure is that the offence must be punishable with imprisonment, without a minimum threshold.

d) Open and clandestine access to stored data

Some of the national reports also discuss the issue of the openness of the search and seizure provisions. The country reports from **Germany** and **Sweden** state that access to data under the search and seizure rules can be carried out only as an open measure.[463] In **Spain** and **France**, if access is not carried out under the remote forensic software provision, the search is also considered an open measure. French legislation requires a search to be carried out "in presence of the person in whose domicile the search is made or of two witnesses,"[464] and Spanish law stipulates that the inhabitant or owner be present.[465]

Clandestine search and seizure are allowed under the legislation of **Australia**, **Belgium**, and the **Czech Republic**. In **Australia**, the TIA Act provides a warrant regime for covert access to stored communications that are in the possession of a service provider. A warrant for such access must be approved by an issuing authority and must satisfy similar thresholds as an interception warrant. However, there are some clear differences, such as a greater number of agencies that can access stored communications, including interception agencies.[466] The **Czech** report states that the clandestine search and seizure of data are permitted under Section 158d Code of Criminal Procedure, which provides for surveillance of persons and items.[467] In **Belgium**, Article 90*ter* CCP (secret interception and secret (network) search) empowers the investigating judge, and in specific cases the public prosecutor, with a purpose, to intercept, to take cognisance of, to search and record

---

[463] See German country report, Chapter III.D.2.e.; Belgian country report, Chapter III.D.2.d. and Swedish country report, Chapter III.C.

[464] French country report, Chapter II.D.2.

[465] Spanish country report, Chapter III.D.2.c.

[466] Australian country report, Chapter III.D.2.

[467] Czech country report, Chapter III.D.2.d.

non-publicly accessible communication or data from a computer system or part of it by technical means, or to extend the search in a computer system or part of it.[468]

3. Duties to cooperate: production and decryption orders

Most of the countries included in this study do not allow an order to provide a decryption key to be addressed to the suspect. The **German** report states that, in this regard, the law of criminal procedure does not provide for any specific rules that would allow requiring the decryption of encrypted data.[469] In **France**, **Hungary**, and **Sweden**, provisions on a duty to cooperate are explicitly not applicable to the suspect.[470] In the **Czech Republic**, according to the national reporter, the provision of a decryption order is not regulated and the practice is uncertain; however, it can be assumed that the requirement for the suspect to provide the decryption key would conflict with the prohibition on self-incrimination.[471]

In **Belgium**, the duty of the suspect to obey an order to provide the decryption key is a matter of current dispute because, while Article 88*quater* Para.2 CCP in relation to a network search provides that the duty to cooperate is not applicable to the suspect, other provisions requiring assistance do not mention the suspect as an exception. Some practitioners thus argue that other forms of cooperation in which decryption is required are permissible concerning a suspect, too.[472]

The **United Kingdom** is the only country in which a suspect can be subject to an order requiring him/her to either "provide information in an intelligible format or to disclose the 'key' to access the protected data."[473] This is not considered self-incrimination in the light of judgement R v S and A [2008] EWCA Crim 2177.[474]

IV. Use of Electronic Communications Data in Judicial Proceedings

In all of the countries, except the **United Kingdom**, the intercepted material, including data obtained abroad, can be used as evidence in criminal proceedings." In the United Kingdom, IPA 2016 (Section 56) prohibits intercepted communications

---

468 Belgian country report, Chapter III.D.1.

469 German country report, Chapter III.D.3.

470 French country report, Chapter III.D.2.; Swedish country report, Chapter III.C.; Hungarian country report, Chapter III.D.3.

471 Czech country report, Chapter III.D.3.

472 Belgian country report, Chapter III.D.3., referring to *Kerkhofs/Van Linthout*, Cybercrime, Politeia, Brussels, 2013, p. 369.

473 UK country report, Chapter III.D.3.

474 Ibid.

being used or disclosed before the courts in civil and criminal proceedings unless certain exceptional circumstances exist. The reason for this prohibition is to exclude the operation of the intelligence and law enforcement agencies from examination. However, even in the United Kingdom, the material obtained through an interception warrant is admissible if it does not reveal anything about the activities of UK law enforcement agencies, such as if the telecommunications operator carries out an interception in order to enforce the provisions of the Communications Act 2003 in accordance with Section 45 IPA 2016.[475]

As far as the issue of the use of preventive or intelligence information in criminal proceedings is concerned, only **Belgian** law explicitly allows data from intelligence services and preventive activities to be used in criminal proceedings.[476] **Spanish** court practice also considers intelligence reports to be admissible as expert evidence in some cases.[477] In **Germany**, the use of such material is generally prohibited under the principle of purpose limitation; however, in some cases, the product of this interception may be admissible if an appropriate measure exists in the law of criminal procedure.[478] In contrast, the **Czech** and **Swedish** reports state that such data are not admissible.[479]

Formal requirements and the provisions on challenging the admissibility of evidence might vary from detailed requirements to very general rules, depending on the jurisdiction. In most of the countries, such rules either fall under the general provisions regulating evidence in criminal proceedings or have been developed in judicial practice concerning the use of the interception product in the courts.

V. Exchange of Intercepted Electronic Communications Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

Mutual legal assistance in lawful interception of electronic communications in the national jurisdictions included in this study is part of a more complex issue of mutual legal assistance in criminal matters. This regime can be governed by international treaties, which a country is a party to, by bilateral agreements on mutual legal assistance, which vary from country to country, and by national legislation in this field.

---

475 UK country report, Chapter IV.

476 Belgian country report, Chapter IV.

477 Spanish country report, Chapter IV.

478 German country report, Chapter IV.

479 Czech country report, Chapter IV, and Swedish country report, Chapter IV.

With regard to the international treaties that provide for mutual legal assistance in the interception of communications, most of the national reports listed such treaties as the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, the Council of Europe Convention on Cybercrime 2001, the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, and the United Nations Convention against Transnational Organised Crime of 15 November 2000. **Belgium** and the **Netherlands** are also parties to the Treaty between the Kingdom of Belgium, the Grand Duchy of Luxembourg, and the Kingdom of the Netherlands concerning extradition and mutual assistance in criminal matters (Benelux Treaty) of 1962.[480]

In addition to international instruments, the countries have various bilateral treaties on mutual legal assistance that aim to further strengthen mutual legal assistance. The number and content of such treaties vary from one country to another. Some of them, such as the supplementary treaties between **Germany** and the **Czech Republic** (2000) and between **Germany** and **Poland** (2003) outline specific rules on the interception of communication, as indicated by the German country report.[481]

The national legislation governing mutual legal assistance in criminal matters includes the following laws:[482]

- **Australia**: Mutual Assistance in Criminal Matters Act 1987
- **Austria**: Federal Law of 4 December 1979 on Extradition and Mutual Assistance in Criminal Matters (ARHG) **and** Federal Law on Judicial Cooperation in Criminal Matters with the Member States of the European Union (EU-JZG)
- **Belgium**: Belgian Act of 9 December 2004 on International Mutual Legal Assistance in Criminal Matters
- **Croatia**: Law on International Legal Assistance in Criminal Matters
- **Czech Republic**: Act No. 104/2013 Sb., on Mutual Judicial Assistance in Criminal Matters
- **France**: Articles 694 et seq. Penal Procedure Code
- **Germany**: Act on International Cooperation in Criminal Matters of 23 December 1982
- **Hungary**: Act XXXVIII of 1996 on International Legal Assistance in Criminal Matters
- **Poland:** Chapters 62, 62a-d, 65 Code of Criminal Procedure

---

480 Belgian country report, Chapter V.A.1.

481 German country Report, Chapter V.A.2.

482 Belgian country report, Chapter V.A.3.; Czech country report, Chapter V.A.3.; French country report, Chapter V.A.1.; German country report, Chapter V.A.1.; Swedish country report, Chapter V.A.; UK country report, Chapter V.

- **Portugal**: Law No. 144/99, of 31 August, on International Judicial Cooperation in Criminal Matters
- **Spain**: Law 23/2014 of 20 November on Mutual Recognition of Criminal Decisions in the European Union
- **Sweden**: Act on International Legal Assistance (2000: 562)
- **United Kingdom**: The Crime (International Co-operation) Act 2003 and IPA 2016

Most of the national reporters also indicate that mutual legal assistance in interception of communications is possible without a bilateral or multilateral treaty: In **Belgium**, the **Czech Republic**, **Germany**, and **Sweden**, according to the country reporters, the national laws providing for general rules on mutual legal assistance enable interception requests on the basis of general clauses. The **Czech** national reporter states that the Ministry of Justice, when addressing such a request, needs to confirm reciprocity, which, according to some, might be preferable for the execution of the request because it allows for less formalities in the procedure.[483] In contrast, the **Swedish** country report remarks that, while the state requesting mutual legal assistance in accordance with Swedish national law need not be party to the treaty acceded to by Sweden, accession to treaties facilitates easier procedures for addressing mutual legal assistance requests.[484]

In the **United Kingdom**, a designated officer appointed by the Secretary of State may issue interception warrants upon application by the competent authority in accordance with an EU mutual assistance instrument or international mutual assistance agreement. These warrants must be issued for the purpose of obtaining communications relating to a person that appears to be outside the UK; or the interception required by the warrant is to take place on premises outside the UK. The statutory duty of the telecommunications operator to give effect to the warrant and the rules on unauthorised disclosure also apply to incoming requests for interception as they apply to targeted interception.[485]

Australia and the **United States** do not intercept upon request of a foreign country.

B. Requirements and Procedure for EU Mutual Legal Assistance, Including Direct Data Transfers

The complex legal regime of international and bilateral treaties, together with the national legislation of a particular country, creates a multifaceted framework of approaches to the incoming and outgoing requests for the interception of communi-

---

[483] Czech country report, Chapter V.A.2.

[484] Swedish country report, Chapter V.A.

[485] UK country report, Chapter V.B.1.

cations. The most harmonised procedure among the states included in this study can be found in the cooperation with the Member States of the European Union under the framework established by the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000. The formal requirements for interception requests are outlined in Article 18 (3) and include the following:

(a) an indication of the authority making the request;

(b) confirmation that a lawful interception order or warrant has been issued in connection with a criminal investigation;

(c) information for the purpose of identifying the subject of this interception;

(d) an indication of the criminal conduct under investigation;

(e) the desired duration of the interception; and

(f) if possible, the provision of sufficient technical data, in particular the relevant network connection number, to ensure that the request can be met.

On the national level, in most of the countries, the competent authorities include either an investigating judge or a prosecutor or both. In some cases, addressing the EU request can also involve participation on the part of the Ministry of Justice.

In **Germany**, the authority responsible for making the decision on whether to respond to the request for mutual legal assistance from an EU Member State is the (head of the) prosecutors' offices at the Regional Courts, acting "in lieu" of the federal authorities.[486] Legislation in some of the federal states grants such a competence to the prosecutors' offices only if the international agreement allows for direct transmission of the mutual legal assistance requests, which is the case for requests received in accordance with the EU Convention 2000 or some of the bilateral treaties with the EU Member States, e.g. those between Germany and the Czech Republic or Poland. The enforcement of the intra-EU requests rests with the same authority that would normally enforce it in domestic cases, meaning that, in the case of an interception, the prosecutors' offices at the Regional Courts must ask the investigating judge at the local court for judicial authorisation. When the local court decides that the request does not meet the requirements for the mutual legal assistance, the Higher Regional Court resolves the case regarding the admissibility of the request.[487]

Like in **Germany** (except for the fact that as a federal state Germany has a more complex system of competence distribution between the federation and the states), the responsible authorities for handling incoming requests in **Austria**, **Belgium**, **Croatia**, **Hungary**, **Italy**, **Poland**, and **Sweden** are the public prosecutor and the investigating judge.[488] Some exceptions from these general rules in **Belgium** in-

---

[486] German country report, Chapter V.B.1.a.

[487] Ibid.

[488] Austrian country report, Chapter IV.B.1.; Belgian country report, Chapter V.B.1.a.; Croatian country report, Chapter V.B.1.; Hungarian country report, Chapter V.C.1.; Italian

clude cases in which regulation requires the request from the EU Member State to be forwarded to the Minister of Justice for consideration if it could be refused under certain conditions provided for in the national law.[489]

In the **Czech Republic**, the legislation defines two stages with regard to the addressing of a request for mutual legal assistance: pre-trial and trial. In the pre-trial stage, the responsible authority is the Department of International Affairs of the Supreme Public Prosecutor's Office, whereas, in the trial stage, the request is processed by the International Department for Criminal Matters of the Ministry of Justice of the Czech Republic.[490] In **Spain**, despite the fact that incoming requests from EU Member States fall under the authority of the competent investigating judge, in practice, the requesting authority might forward it to the National Court, which has jurisdiction over the entire territory. Sometimes, the mutual legal assistance requests also land in the International Cooperation Unit of the Public Prosecutor's Office, which forwards it to the investigating judge.[491]

As regards outgoing requests, the national system mirrors the regulation for addressing incoming requests. For example, in **Austria**, **Croatia**, the **Czech Republic**, **Germany**, and **Hungary**, preparation of a request for the interception of communications in another EU Member State is completed by the public prosecutor, but in **Spain**, where many responsibilities for addressing mutual legal assistance requests rest with judiciary authorities, it is up to the investigating judge, who is responsible for sending the request.[492]

One of the most complex issues related to EU cooperation on the interception of communications concerns direct data transfers. While Articles 18 and 19 of the EU Convention on Mutual Assistance in Criminal Matters 2000 enable such transmissions, more than a decade after the adoption of this instrument, direct transfers are rarely used in practice, and the national approaches to this matter vary significantly. While the **Czech** and **German** national reporters refer to the possibility of direct data transfers in accordance with their national legislations,[493] the **Spanish** country report states otherwise. The Spanish national report notes that the current national legal framework and technical regulations do not enable law enforcement agencies from another EU Member State to "have direct access to the data resulting from the telecommunications interception."[494] Other countries, like **Sweden**, according to

---

country report, Chapter V.B.1.; Polish country report, Chapter V.B.1.; Swedish country report, Chapter V.B.

489 Belgian country report, Chapter V.B.1.a.

490 Czech country report, Chapter V.B.1.

491 Spanish country report, Chapter V.B.1.

492 Austrian country report, Chapter IV.B.2.; German country report, Chapter V.B.2.; Croatian country report, Chapter V.B.2.; Czech country report, Chapter V.B.2.; Hungarian country report, Chapter V.C.; Spanish country report, Chapter V.B.2.

493 Czech country report, Chapter V.B.4.; German country report, Chapter V.B.4.a.

494 Spanish country report, Chapter V.B.4.

the national report, require some technical, legal, and organisational national reform measures to perform direct data transfers. However, according to the national reporter, Swedish law does not have to undergo any major reforms to enable direct transfers if there is mutual trust.[495]

Thus, despite the existence of the international framework and – in some countries – national regulation enabling direct transfers, both the national reports and the workshops with law enforcement agency representatives revealed that, in practice, such transfers rarely take place. For example, the Czech national reporter commented that, although the law permits direct transfers, the "Czech Republic is poorly prepared for such a solution and subsequent transfers are mostly used."[496] Most of the jurisdictions included in this study do not execute such transfers on a regular basis or, even if they are performed, the law enforcement authorities still encounter problems, e.g. an unexpected cut in direct transfers in the middle of an intercepted conversation. Instead of direct data transmissions, the national law enforcement authorities use different ways of handling intercepted material – from downloading it safely to the FTP servers to sending it to hard drives or other mediums.

C. European Investigation Order

One of the major issues addressed by all the national reporters of the EU Member States is the question of whether Directive 2014/41/EU regarding the European Investigation Order in criminal matters would significantly change mutual legal assistance in the interception of communications. At the time of writing this comparative report, the European Investigation Order directive was transposed into the national legislation of all of the European Union jurisdictions included in this study. Some national reporters – such as the **German** reporter – expressed the opinion that the new regulation cannot significantly challenge or influence the current complex regime of mutual legal assistance in the matter of interception requests.[497]

---

[495] Swedish country report, Chapter V.B.

[496] Czech country report, Chapter V.B.4.

[497] Czech country report, Chapter V.C.; German country report, Chapter V.C.

List of Abbreviations

BND	Bundesnachrichtendienst (German Federal Intelligence Service)
CCP	Belgian Code of Criminal Procedure
CJP	Swedish Code of Judicial Procedure
CNI	Centro National de Inteligencia (Spanish National Intelligence Centre)
CZK	Czech currency
DRIPA	Data Retention and Investigatory Powers Act
ECA	Swedish Electronic Communications Act
ECJ	European Court of Justice
FRA	Försvarets radio anstalt (Swedish National Defence Radio Establishment)
GCHQ	Government Communications Headquarters (British signal intelligence service)
IAP	Internet Access Provider
ICT	Information and Communication Technology
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISP	Internet Service Provider
LEA	Law Enforcement Agency
LECRIM	Ley de Enjuiciamiento Criminal (Spanish Criminal Procedure Code)
LOPPSI	Loi d'orientation et de programmation pour la sécurité intérieure (French Law on Orientation and Programming Performance of Homeland Security)
MAD	Militärischer Abschirmdienst (German Military Counter-intelligence Service)
PACE	British Police and Criminal Evidence Act
PTS	Post och telestyrelsen (Swedish Post and Telecom Authority)
RIPA	Regulation of Investigatory Powers Act
SIM	Intelligence and security services
SMS	Short Message Service
SOU	Statens offentliga utredningar (Swedish Government Official Reports)
StGB	Strafgesetzbuch (German Criminal Code)

StPO	Strafprozessordnung (German Code of Criminal Procedure)
TKG	Telekommunikationsgesetz (German Telecommunications Act)
TKÜV	Telekommunikations-Überwachungsverordnung (German Telecommunications Interceptions Ordinance)
TR TKÜV	Technische Richtlinie TKÜV (German Technical Directive TKÜV)
VoIP	Voice over Internet Protocol

Part 3
Country Reports

Australia*

National Rapporteur:
Catherine Smith

* This report outlines the legislation and case law as of February 2019.

Contents

I. Security Architecture and the Interception of Telecommunication

The Commonwealth of Australia is a federation made up of 6 States and 2 Territories, laws for Australia are made at both the Commonwealth and State or Territory level. The Australian *Constitution Act 1901* (the Constitution) provides for the legislative power of the Australian Parliament. Under the Australian Constitution laws are developed at a Commonwealth or Federal level and apply to the whole of Australia. The States and Territories also create laws for their governance, including for policing. The *Telecommunications (Interception and Access) Act 1979* (TIA Act), is the primary law relevant to this report and was passed by the Commonwealth Parliament in 1979 and is administered by a Commonwealth Minister.[1] States and Territories are afforded procedural powers under the TIA Act but also work under their own criminal law. For the purposes of this report the answers will be limited to the Commonwealth law with any necessary references to State or Territory law.

There is very little if any case law on the interpretation of the TIA Act, nor is there significant academic comment. The TIA Act has been amended significantly in the last 10 years and most commentary relates to opposition or discussion on the proposed amendments. The most significant analysis of the TIA Act can be found in reports of various Parliamentary Committees that have reviewed draft amendments to the Act.[2]

A. Law Enforcement Institutions and Security Services with Powers of Telecommunication Interception

1. National security architecture

In Australia the Australian Security Intelligence Organisation (ASIO) is the key agency for Australia's domestic national security. The Australian Security Intelli-

---

[1] Until recently the Act was administered by the Attorney-General, it is now administered by the Minister for Home Affairs.

[2] Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 27 February 2015 © Commonwealth of Australia 2015 ISBN 978-1-74366-270-0 (Printed version) ISBN 978-1-74366-271-7 (HTML version) and Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 December 2018 © Commonwealth of Australia 2018 ISBN 978-1-74366-944-0.

gence Service (ASIS) is Australia's overseas secret intelligence collection agency and the Australian Signal Directorate is the signals intelligence agency. All these agencies are established under legislation which details functions and roles.[3]

As noted, Australia is a federation and as such has both national and state level police forces with some powers and offences applying in both federal and state jurisdictions. The Australian Federal Police is Australia's national police agency and the Australian Criminal Intelligence Commission is Australia's national criminal intelligence agency. Both these agencies work with and separately from the Police agencies that are based in Australia's States and Territories. There are currently 18 interception agencies in Australia including ASIO, the AFP, ACIC, State and Territory police agencies, crime commissions and integrity or anti-corruption agencies.

2. Powers for the interception of telecommunication

The TIA Act provides the framework for all interception of telecommunications in Australia. This Act is complemented by Commonwealth and State surveillance device legislation and Part 14 of the Telecommunications Act 1997 (Telecommunications Act), which deals with National Interest matters.

a) Law of criminal procedure

The police may only use telecommunications interception in the investigation of criminal offences. Generally, the offence must be a serious offence that is punishable by imprisonment for life or for a period, or maximum period, of at least 7 years.[4]

There are some exceptions to this threshold, usually relating to offences that by nature are online and interception is likely to be the only form of evidence available to the investigator, for example some cybercrime offences. Section 5D of the TIA Act provides clear direction on the types of offences that may be investigated with the use of telecommunications interception.

b) Preventive law

The TIA Act does not as a rule provide for interception by the police agencies as a preventative measure, however, there is an exception relating to an interception warrant issued where a control order is in place. If a control order is in place an agency may apply for a telecommunication service or named person warrant where the information obtained may substantially assist

---

[3] *Australian Security Intelligence Act 1979* and the *Intelligence Services Act 2001.*

[4] Section 5D TIA Act.

the protection of the public from a terrorist act; or preventing the provision of support for, or the facilitation of, a terrorist act; or preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or determining whether the control order, or any succeeding control order, has been, or is being, complied with).[5]

c) Law of intelligence agencies

ASIO may apply for a warrant to intercept communications where a person is engaged in, or reasonably suspected by the Director-General of Security[6] of being engaged in, or being likely to engage in, activities prejudicial to security.[7] ASIO may also apply for a warrant to intercept communications to enable the collection of foreign intelligence relating to matters in the interests of Australia's national security, Australia's foreign relations or Australia's economic wellbeing. ASIO's collection of telecommunications interceptions is not evidential and is generally used for intelligence purposes.

d) Customs Investigation Service

The Australian Border Force is not an interception agency, however offences under the *Migration Act 1958* are offences to which telecommunications interception applies.

3. Responsibility for the technical performance of interception measures

Australian law places various obligations upon a carrier and a carriage service provider (service providers) to provide reasonably necessary assistance to law enforcement and national security agencies, which includes the provision of interception services, including services in executing an interception warrant.[8]

In addition, the TIA places requirements on service providers to develop interception capability and delivery capability to facilitate the technical execution of a warrant and the delivery of the intercepted material to a point agreed by the agencies. Recent amendments to the Telecommunications Act introduced a range of technical assistance requirements, these will be discussed later in the chapter.

---

[5] Control orders are part of Australia's anti-terrorism legal framework, interception warrants for control orders are issued under sections 46 and 46A TIA Act.

[6] The Director-General of Security is the Chief officer of ASIO.

[7] Part 2-2 TIA Act.

[8] Subsection 313 (3) and (7) *Telecommunications Act 1997* are significant provisions as they provide the framework for seeking the assistance of carriers and carriage service providers.

4. Legitimacy of data transfers between different security agencies

Section 19A ASIO Act provides for that agency to cooperate with intelligence and law enforcement agencies in connection with the performance of their functions. These amendments were introduced in 2011 with the stated purpose of providing for greater flexibility for ASIO to share information obtained in the performance of its functions with other Australian intelligence agencies and with the broader national security community.[9]

The TIA Act provides for the exchange of lawfully intercepted information between agencies including if it is found that the information relates or appears to relate to activities prejudicial to security, the commission of a relevant offence, specified disciplinary matters, or where the information may give rise to an investigation.[10] Section 68 TIA Act envisages situations where one agency has intercepted material relevant to an investigation or possible investigation being carried out by another agency. In addition, section 67 TIA Act allows the sharing of information to further progress an investigation, this is called a 'permitted purpose.'[11] This provision includes sharing information in a joint investigation, with a forensic specialist or with a prosecutor, it does not envisage the information being used for a purpose other than for which is was shared.

B. Statistics on Telecommunication Interception

1. Obligation to collect statistics

There is an obligation on agencies to retain documents and records in connection with interception for the purposes of the Ombudsman's inspections.[12] The obligation to retain these records is contained in both the TIA Act and State and Territory legislation. In addition, the Secretary of the Department responsible for administering the TIA Act, must create a General register and a Special register of warrants, which contains details of all warrants issued to agencies, except ASIO. These registers are provided to the Minister for inspection but are not made publicly available.[13]

---

[9] *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011.*

[10] Section 68 TIA Act provides an exhaustive list of circumstances where lawfully intercepted information may be communicated to another agency.

[11] Permitted purpose is defined in section 5 TIA Act and specifies a broad range of functions that interception may be used for.

[12] The Commonwealth Ombudsman in established under the *Ombudsman Act 1976*. The Ombudsman has a significant inspection role for many of the Commonwealth agencies powers under the TIA Act and *Surveillance Devices Act 2005*.

[13] Requirements to retain this information are contained in Part 2-7 TIA Act, Keeping and inspection of interception records.

All intercepting agencies except ASIO, must provide annual reports to the relevant Minister. The report includes details of applications made and warrants issued under Part 2-5 TIA Act. In addition, a Managing Director of a carrier must also provide an annual report to the Minister. The Minister will then provide an Annual Report to Parliament on the details of those warrants issued under Part 2-5. ASIO reports to the Attorney-General on each warrant issued under Part 2-2 TIA Act.

2. Current data

The Annual Report for the year 2017/2018 has not yet been tabled in Parliament. The most recent statistics relate to the report for the 2016/2017 year.[14] The annual report breaks down the statistics into categories of warrant and provides details on the offences, prosecutions and convictions. The Annual Report disclosed there were 3,717 interception warrants issued across 17 interception agencies, not including warrants issued to ASIO as they have no obligation for public reporting. There were also 674 warrants issued for access to stored communications, a communication that is stored by a service provider. In the same reporting year, 20 enforcement agencies made 300,224 authorisations for the disclosure of information or a document from a service provider.

II. Principles of Telecommunication Interception in Constitutional and Criminal Procedural Law

A. Constitutional and Other Legislative Safeguards of Telecommunications

1. Areas of constitutional protection

Unlike in many other countries, Australia's Constitution does not contain protections for human rights or privacy, but rather it establishes the framework for how Australia is governed. Section 51 Constitution provides the Commonwealth with the power to 'make laws for the peace, order, and good government of the Commonwealth' with respect to specific heads of power. There is no head of power related to privacy or secrecy. There is no general right to privacy in Australian law, however there is privacy legislation which protects certain information by placing obligations on government agencies and some private sector organisations – the *Privacy Act 1988* – which will be discussed further below.

---

[14] Telecommunications (Interception and Access) Act 1979 Annual Report 2016–17 ISBN 978-1-920838-32-4 (print) ISBN 978-1-920838-33-1 (online).

2. Proportionality of access to data

Privacy and proportionality tests are a requirement for any application for access to data, whether interception, stored communications or subscriber data. These are not based on constitutional laws but within the TIA Act. When considering an application for an interception warrant, the Issuing Authority must have regard to several matters that ensure that the issue of the warrant is proportionate to the offence being investigated:[15]

– how the privacy of any person or persons would be interfered with by interception under a warrant…

– the gravity of the conduct constituting the offence or offences being investigated…

– to what extent methods of investigating the offence or offences that do not involve so intercepting communications have been used…[16]

3. Consequences for the interception of telecommunication

a) Protection of the secrecy of telecommunications

It is an offence under Australian law for a person to intercept or access private telecommunications without the knowledge of those involved in that communication.

Section 7(1) TIA Act provides:

(1) A person shall not:
  a) intercept;
  b) authorize, suffer or permit another person to intercept; or
  c) do any act or thing that will enable him or her or another person to intercept;
  d) a communication passing over a telecommunications system.

There are exceptions to the offence specifically for law enforcement and national security agencies to intercept telecommunications under lawful authority or in a risk to life situation. An employee of a service provider who is in the lawfully engaged in their duties is also exempt. However, it is an offence to deal with intercepted material in contravention of the TIA Act.[17] An offence committed under these sections is punishable on conviction by imprisonment for a period not exceeding 2 years.[18] The TIA Act provides for both civil and criminal remedies where a per-

---

[15] An Issuing Authority is defined in the TIA Act as eligible Judge or nominated Administrative Appeals Tribunal member.

[16] Section 46 TIA Act provides the test to be applied for the issue of a telecommunications service warrant.

[17] *Ibid*. section 63.

[18] *Ibid*. section 105.

son has unlawfully intercepted another's communications. The relief provided is at the discretion of the court but may include monetary or injunctive relief.[19]

b) Protection of the confidentiality and integrity of information systems

Australian law has a robust approach to the protection of any information held on a communications network. Part 13 Telecommunications Act requires the confidentiality of information that relates to the contents of communications, carriage services supplied by carriers and carriage service providers; and the affairs or personal particulars of other persons.[20] The obligation falls upon service providers, number database operators, emergency call operators and their respective associates.

It is a criminal offence to have unauthorised access to data held on a computer; to modify data without authorisation; or to modify data to cause impairment of electronic communications. These are criminal offences that are punishable with between 2 and 10 years' imprisonment, depending of the seriousness of the offence.[21]

4. Statutory protection of personal data and protection of professional secrets in criminal procedural law

As noted, Australia has a Privacy Act that regulates how personal information is handled by most Australian government agencies and all private sector organisations with an annual turnover of more than $3 million (this includes carriers and some carriage service providers). The Privacy Act defines personal information as:

> …information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.[22]

The Federal Court has ruled in relation to a case dealing with access to telecommunications data, that personal information requires

> an evaluative conclusion, depending on the facts of any individual case' and that 'even if a single piece of information is not 'about the individual' it may be about the individual when combined with other information.[23]

In September 2018 a new regulatory framework commenced in Australia that requires carriers and carriage service providers to endeavour to protect networks and facilities from unauthorised access and interference. When passed the legislation had the stated purpose

---

19 Section 107A TIA Act.

20 Part 13 *Telecommunications Act 1997.*

21 Part 10.7 *Criminal Code Act 1995* deals with computer offences, State and Territories also legislate for computer offences.

22 Privacy Act 1988.

23 *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 at [65].

to better manage national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities.[24]

B. Powers in the Code of Criminal Procedure

1. Requirement of (reasonable) clarity for powers in the law of criminal procedure

Police investigations follow a common law system in Australia with the police undertaking an investigation to collect evidence. The police use powers available to them under either Commonwealth or State and Territory criminal law or by specific powers found in standalone legislation such as the *Surveillance Devices Act 2004* (SD Act), the TIA Act or agency-specific Acts. There is no one rule on how evidence is collected, how to access coercive powers or how an investigation is managed. For example, section 3F *Crimes Act 1922* has specific provisions that deal with search warrants and what can and cannot be done in the course of a search and the Australian Criminal Intelligence Commission may under its legislation, the *Australian Crime Commission Act 2002* compel a person to give evidence for the purposes of their special operations or investigations.

2. Differentiation and classification of powers in the law of criminal procedure

Australian legislation is precise in the requirements necessary to satisfy a Judge, magistrate or issuing authority of the need to access coercive powers. The Police are required to act in accordance with the relevant law and are generally subject to accountability and oversight for covert powers. The thresholds for police procedural powers differ depending on the power and the extent to which it may breach the rights of the person or persons affected by executing the warrant or authorisation. Interception is a warrant of last resort and has the highest threshold for access. In recent years, amendments to legislation that introduce new coercive powers have a level of consistency, including who may issue the warrant, the need for the application to be proportionate to the gravity of the offence, the need to consider the privacy of persons affected and the need for oversight.

---

[24] Telecommunications and Other Legislation Amendment Act 2017 – Revised Explanatory Memorandum circulated by authority of the Minister for Home Affairs, the Hon Peter Dutton MP.

III. Powers for Accessing Telecommunication Data in the Law of Criminal Procedure

A. Overview

The TIA Act provides for interception of communications. The Act empowers 18 intercepting agencies to apply for a warrant to intercept communications in their passage over a telecommunications system. The TIA Act also provides for the collection of stored communications, access to information or documents (telecommunications data) held by service providers and data retention. Part 2-2 contains the statutory provisions for ASIO to intercept telecommunications and Part 2-5 contains the provisions for agencies to interception telecommunications.

B. Interception of Content Data

1. Statutory provision

There are several statutory provisions relevant to the interception of communications under Australian law. Law enforcement interception may only take place under a warrant for the investigation of a serious offence as defined in section 5D TIA Act. A warrant may only be issued by an eligible Judge or nominated Administrative Appeals Tribunal member (issuing authority). Section 39 provides the power for an agency to apply for a warrant to intercept the communications of a service or a person:

> s39(1) An agency may apply to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service or a person…

Section 40 TIA Act requires the application be in writing but allows for an application to be made by phone in urgent circumstances. Section 42 TIA Act requires an affidavit to be made as part of the application and for it to establish the grounds for the warrant being sought. Division 4, Part 2-5 TIA Act deals with the 4 forms of interception warrant available to agencies, these are section 46 ‘telecommunications service warrant’, section 46(1)(d)(ii) ‘B-Party warrant, section 46A ‘named person warrant’ and section 48 ‘warrant for entry on premises’ (this is only available for the interception of a service not a person). Before a warrant is issued, an issuing authority must be satisfied on several matters in relation to the investigation, including the likely effectiveness of the warrant.

2. Scope of application

a) Object of interception

Section 6(1) TIA Act defines interception of a communication as:

> s6(1) For the purposes of this Act, but subject to this section, interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

A communication is defined in section 5 as:

> **communication** includes conversation and a message, and any part of a conversation or message, whether:
> (a) in the form of:
> (i) speech, music or other sounds;
> (ii) data;
> (iii) text;
> (iv) visual images, whether or not animated; or
> (v) signals; or
> (b) in any other form or in any combination of forms.

A warrant issued under section 46 allows interception of a telecommunications service of a particular person or another person with whom the target of interest is likely to communicate. A service is defined in section 5 as:

> service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radiocommunication.

A warrant issued under section 46A allows an agency to intercept a person's communications made to or from a telecommunications service or using a telecommunications device. A telecommunications device is defined in section 5 as:

> means a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system.

The definition of what constitutes an interception is broad and technologically neutral with its application to any form of communication that travels on a telecommunications system. The definition of communication is also broad enough to include any form of communication, including:

- analogous communication (voice and data);
- IP-traffic of a person-to-person-communication;
  - IP-traffic between a person and an automated information system;
  - IP-traffic between a person's computer and their data storage in a cloud or other remote storage of data processing systems IP-traffic between two independent computer systems.

b) Temporal limits of telecommunication

A communication that is no longer passing over a telecommunications system is called a 'stored communication.' The TIA Act prohibits unlawful access to a stored communication unless prescribed under section 108. Criminal law-enforcement agencies, including the Australian Border Force, may access stored communications under a warrant.

3. Special protection of confidential communication content

An interception warrant authorises the interception of all communications made to or from a telecommunications service or by means of a telecommunications device. It is open to the issuing authority to specify conditions or restrictions or exclude a telecommunications service to limit the authority conferred by the warrant. The TIA Act allows the collection of the whole communication and this would include communications that may be defined as privileged, however this does not mean that the privileged communications may be used in an investigation or as evidence. In Australia the definitive law on legal professional privilege is found in a decision of the High Court:

> Legal professional privilege is not merely a rule of substantive law. It is an important common law right or, perhaps, more accurately, an important common law immunity. It is now well settled that statutory provisions are not to be construed as abrogating important common law rights, privileges and immunities in the absence of clear words or a necessary implication to that effect.[25]

The full Federal Court has held that

> …legal professional privilege is not destroyed if a privileged communication is intercepted pursuant to a warrant issued under the TI Act. In particular, the privilege survives so as to render the intercepted communications inadmissible in subsequent proceedings.[26]

It will be a matter for the agency to determine whether the intercepted communication is privileged and as such afforded protection. The mere existence of the communication would not in itself be privileged.[27]

4. Execution of telecommunication interception

a) Execution by the authorities with or without the help of third parties

A warrant issued to an agency under section 46 or 46A does not authorise the interception of communications unless a carrier is notified of the warrant and provid-

---

[25] *Daniels Corporation International Pty Ltd v Australian Competition and Consumer Commission* (2002). 213 CLR 543, [11].

[26] *Carmody v Mackellar* (1997) 148 ALR 210.

[27] *National Crime Authority v S* [1991] FCA 234.

ed with a certified copy (section 47 TIA Act).[28] An interception warrant authorises the interception of communications as they pass over the Australian telecommunications system. A carrier is obliged to undertake the technical aspects of the interception on behalf of the agency.

Section 48 TIA Act is an exception to the rule in that an interception warrant may be issued to permit entry on premises. A warrant will be issued where there are technical reasons connected with the interception that require it to be done on a premises rather than by a carrier. When issuing a warrant under this provision the Issuing Authority must be satisfied that it would be

> impracticable or inappropriate to intercept communications … other than by the use of equipment or a line installed on those premises.[29]

b) Accompanying powers for the execution of interception

In late 2018, the Australian Parliament passed the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018*.[30] This Act introduced new laws including Computer Access Warrants (CA warrant) and technical capability notices (the latter will be addressed later in the chapter). The new CA warrant came into force on 9 December 2018 and at the time of writing there is no commentary available on its use. The Act amends the *Surveillance Devices Act 2004* (SD Act) to allow agencies

> to covertly access devices to investigate serious crimes, to search devices such as laptops, mobile phones and USBs, and collect information and to conceal the fact that a device has been accessed.[31]

During the passage of the legislation, supporting documentation stated:

> Computer access is a valuable in the current digital environment because it allows officers to access data held on a device in an unencrypted state.[32]

A CA warrant may also be used after an international assistance request is received from a foreign country.

---

[28] A carrier is a carrier and a carriage service provider as defined in the Telecommunications Act.

[29] Subsection 48(3)(d)(ii) TIA Act.

[30] The Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018 is currently undergoing a review by the Parliamentary Joint Committee on intelligence and Security with a reporting date of 3 April 2019.

[31] Paragraph 19, Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 Explanatory Memorandum, circulated by authority of the Minister for Home Affairs, the Hon Peter Dutton MP.

[32] *Ibid*., paragraph 71.

5. Duties of telecommunication service providers to cooperate

a) Possible addressees of duties of cooperation

As noted, carriers and carriage service providers (service providers) are required to provide reasonably necessary assistance to agencies, including in the execution of an interception warrant. Section 313(3) Telecommunications Act 1997 is the basis of this obligation and includes assistance in enforcing the criminal law and laws imposing pecuniary penalties; assisting the enforcement of the criminal laws in force in a foreign country; assisting the investigation and prosecution of crimes within the jurisdiction of the *International Criminal Court*; Tribunal offences under the *International War Crimes Tribunals Act 1995*; protecting the public revenue; and safeguarding national security.

In addition, subsection 313(7) provides inter alia:

> (7) A reference in this section to giving help includes a reference to giving help by way of:
>
> a) the provision of interception services, including services in executing an interception warrant under the Telecommunications (Interception and Access) Act 1979; or
>
> b) giving effect to a stored communications warrant under that Act; or
>
> c) providing relevant information about:
>
> (i) any communication that is lawfully intercepted under such an interception warrant; or
>
> (ii) any communication that is lawfully accessed under such a stored communications warrant; …

The requirement to assist is broad and before approaching a service provider for assistance an agency must be satisfied that the service provider falls within the definition of carrier or carriage service provider. A carriage service provider will include service providers who offer or propose to offer a service to the public using a network unit owned by one or more carriers or a network unit in relation to which a nominated carrier declaration is in force. Essentially any service provider who offers a service in Australia could be approached to provide reasonably necessary assistance and this may include foreign service providers.

The Telecommunications Act was amended in December 2018 to introduce an additional regime for cooperation. The amendments introduce a 3-tiered regime for assistance from a ‘designated communications provider.’ A designated communications provider is defined in section 317C Telecommunications Act and includes a broader range of service providers than previously assisting under section 313 of the Act, including foreign and domestic communications providers and device manufacturers. The supporting documentation to the amending Act notes that these amendments will assist with the challenges law enforcement face from encrypted technologies.

b) Content of duties to cooperate

Assistance under section 313 Telecommunications Act regulates to the level noted above. The Telecommunications Act establishes a framework for cooperation under a technical assistance request (TAR), a technical assistance notice (TAN) or a technical capability notice (TAC). Any assistance must be 'reasonable and proportionate' and is also 'practical and technically feasible.'[33] In addition, the requests are time limited and a service provider may be compensated for the assistance.

There are three types of assistance: A TAR is voluntary assistance sought from an agency and agreed to by a designated communications provider; a TAN is a compulsory notice where it is established a provider can assist within their capabilities but does not agree to do so on a voluntary basis. In this case an agency will issue a TAN, but it cannot require a provider to build a capability for compliance with the notice; a TCN is a compulsory notice where the provider does not wish to provide the assistance voluntarily and the provider may be required to build capability to meet the notice.

The Section 317E Telecommunications Act describes a list of 'acts or things' that may be done under the request and notices, the list is exhaustive for the purposes of the compulsory powers but is not for voluntary assistance.

c) Duties to provide technical and organisational infrastructure

The TIA Act regulates the terms of the assistance required for interception and delivery capabilities. The responsible Minister may, by legislative instrument, determine a specific interception capability which is based on an international standard or guideline. At the time of writing there does not appear to be any determination in place. Regardless of a determination, section 191 TIA Act places obligations on service providers to have interception capability that will enable the execution of a warrant and to transmit the intercepted information to a delivery point. This obligation includes a requirement to ensure that capability is developed, installed and maintained. A service provider may apply for an exemption from their requirements under this section.

The TIA Act includes a regime for carriers and nominated service providers to provide an interception capability plan (ICP) to the Communication Access Coordinator (CAC).[34] An ICP is an annual statement by a carrier or nominated carriage service provider on strategies to manage interception capabilities on all services

---

[33] Sections 317JAA, 317P and 317V.

[34] The CAC is an administrative role within the Department of Home Affairs, responsible for administering the TIA Act, the CAC is a point of liaison between agencies and service providers on issues under the TIA Act and the Telecommunications Act.

that are offered by the provider, as well as a statement on how and where the provider intercepts communications, including for new services. The ICP must also list employees responsible for interception and include a statement that the provider will comply with their legal obligations to provide interception capabilities.

The TIA Act divides the financial responsibility for the technical requirements of interception between the agencies and service providers. Sections 207 and 208 TIA Act respectively provide:

> The capital and ongoing costs of developing, installing and maintaining a capability imposed on a carrier under section 190 or 191 in respect of a particular kind of telecommunications service are to be borne by the carrier.
>
> The capital and ongoing costs, worked out in accordance with section 209, of developing, installing and maintaining a delivery capability imposed on a carrier under Part 5-5 in respect of a particular kind of telecommunications service are to be borne by the interception agency concerned.

d) Security requirements for data transfers by communication service providers

The CAC may make a determination on delivery capability, including the format of the information, the point and manner it is delivered and any ancillary information that should accompany that information. The determination is not a public legislative instrument, so at the time of writing there are no details available on whether a determination has been made. The Act also covers persons not covered by a determination and that person must ensure that they have a delivery capability that is developed, installed and maintained.[35]

Procedures for accessing electronic evidence for a foreign State are managed under both the TIA act and the *Mutual Legal Assistance in Criminal Matters Act 1987* (MLACM Act). Australia does not intercept communications on behalf of a foreign State, however access to already collected intercept product is available in limited circumstances. The sharing of electronic evidence is discussed in detail later in the chapter.

6. Formal prerequisites of interception orders

a) Competent authorities

An issuing authority may issue a warrant for the interception of communications. The responsible Minister must appoint an issuing authority before they may hear an application to issue a warrant. Issuing authorities must consent to be appointed to this role. The Attorney-General may issue a warrant to ASIO for the interception of communications. The TIA Act allows for warrant applications to be made to an issuing authority in an emergency but only in limited circumstances. As noted ear-

---

[35] Part 5-5 TIA Act.

lier there are 17 interception agencies (law enforcement or corruption not including ASIO) who may apply for warrants. They include the Australian Commission for Law Enforcement Integrity, the Australian Criminal Intelligence Commission, the Australian Federal Police, the Corruption and Crime Commission (Western Australia), the Crime and Corruption Commission (Queensland), the Independent Broad-based Anti-Corruption Commission (Victoria), the Independent Commission Against Corruption (New South Wales), the New South Wales Crime Commission, the New South Wales Police Force, the Northern Territory Police, the Law Enforcement Conduct Commission, the Queensland Police Service, the Independent Commissioner Against Corruption (South Australia), the South Australia Police, the Tasmania Police, the Victoria Police and the Western Australia Police.

All State or Territory interception agencies were required to seek the Minister's declaration to be an intercepting agency under the TIA Act.

b) Formal requirements for applications

An application for an interception warrant must be in writing and made by a member of the relevant law enforcement agency or a member of staff of other agencies. In urgent circumstances a warrant may be made by telephone, by a chief officer of an agency or a person authorised by the chief officer to make the application. The written application must provide the name of the agency and the name of the person making the application.

c) Formal requirements for orders

The application must be accompanied by an affidavit which details the facts and other grounds for the application. The affidavit will also include the proposed duration of the warrant, details of previous applications, number of previous warrants issued, and the use made of any information previously provided under warrant. If the application is for a named person warrant the affidavit must set out the name or names by which the person is known, (this may include an alias); details of the service being used, (to the extent they are known); and if a device is to be intercepted, details of the device.[36] If an application is made by telephone the applicant must provide the same information over the phone and include details as to why the application is urgent and follow up the application with an affidavit within one day.

An issuing authority may require further information before deciding the application, which may be given orally or in writing as directed and shall be given on oath. In the case of Queensland and Victoria (State jurisdictions), there is a further formal requirement for the application of an interception warrant. Both states have

---

[36] Section 42 TIA Act.

a Public Interest Monitor (PIM) who can make submissions, orally or in writing, on matters that the issuing authority shall have regard to in issuing a warrant.

7. Substantive prerequisites of interception orders

a) Degree of suspicion

The degree of suspicion required to apply for an interception warrant is that a person is using or likely to use the service or device and communications would be intercepted under the warrant. In addition, information obtained under the interception

> would be likely to assist in connection with the investigation by the agency of a serious offence, or serious offences, in which the person is involved (section 46(1)(d) and section 46A(1)(d) TIA Act).

In circumstances where the police reasonably believe that the person of interest is communicating with another person in the commission of an offence then the other person's phone may be intercepted (B-Party warrant). In the case of a B-Party warrant, the issuing authority must be satisfied that a person of interest is communicating with the person who uses the service.[37]

b) Predicate offences

An interception warrant is available for the interception of a serious offence. A serious offence is defined in section 5D TIA Act and covers a broad range of general and specific offences, including but not limited to murder, terrorism, money laundering, offences related to criminal organisations and drug offences. All offences must link back to a federal, state or territory law. An important threshold for most of the offences is that it is punishable by imprisonment for life or for a period, or maximum period, of at least 7 years.

There are a few offences that do not meet the 7-year threshold, and these include cybercrime offences. The nature of cybercrime is that offences exist in the online environment and have no detectable offline presence, so interception is often one of the more effective tools of investigation.

c) Persons and connections under surveillance

The nature of interception law in Australia is that the warrant will be sought to obtain evidence about a person who is believed to be engaged in behaviour that justifies the issue of a warrant. A warrant will authorise the interception of communications on services or devices a person is using or believed to use or the ser-

---

[37] Section 46(1)(d)(ii).

vice of another person, where it is believed the person of interest in likely to contact them.

– *Principle of subsidiarity*

Interception warrants for criminal investigations are issued to intercept a person or a telecommunications service, this includes the interception of a device.

d) Proportionality of interception in individual cases

Before issuing a warrant, an Issuing Authority must have regard to several matters addressing the proportionality of the application. These include the extent to which the privacy of a person or persons would be interfered with as a result of the interception; the seriousness of the conduct involved in the offence or offences; the usefulness of the information in investigating the offence and the extent that interception will assist in the investigation; what alternative methods of investigation have been used or could be used; and whether the use of interception would be likely to prejudice the investigation, whether because of delay or for any other reason (sections 46(2) and 46A (2) TIA Act).

e) Consent by a communication participant to the measure

Interception of a communication is prohibited without the knowledge of the parties to the communication. It is usual practice in Australia for businesses to provide callers with a recorded message that their communication is being recorded to ensure they are not breaching the TIA Act. The TIA Act has a provision (section 30) that enables the interception of communications to trace a person in an emergency where another person (whether a police officer or not) has received a call and as a result of that call is concerned that there is a risk to life and the location of the person is unknown. The TIA Act also provides exceptions to the prohibition against interception where an officer of an agency is party to a communication or where the person to whom the communication is directed has consented to the interception, and there are reasonable grounds for suspecting another party to the communication has acted in such a way to raise suspicion of a:

> loss of life or the infliction of serious personal injury; or threatened to kill or seriously injure another person or to cause serious damage to property; or threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or safety (section 7(4) and (5) TIA Act).

As soon as practicable after the interception under these subsections, an officer of an agency must make the application for the interception warrant.

8. Validity of interception order

a) Maximum length of interception order

An interception warrant is issued for a period of up to 90 days except in the case of a B-Party warrant, which is issued for up to 45 days. A warrant issued in an emergency is subject to the same time limits. An Issuing Authority may not vary the period of a warrant by extending the period but may issue a warrant for a shorter period.

b) Prolongation of authorisation

It is open to an agency to apply for a renewal of an interception warrant. By virtue of the definition of 'renewal application', an application is made before the expiry of the previous warrant. There is no automated approval of a renewal application, with agencies required to follow the same steps as they would in an initial application including information on how the continued interception is likely to assist with the investigation. As an affidavit is provided with the renewal application, it is open to the agency to provide details in writing on what evidence of the offence has been identified.[38]

c) Revocation of authorisation

A chief officer of an agency may revoke a warrant at any time. In addition, the chief officer of an agency must revoke a warrant if he or she is satisfied that the grounds for the warrant no longer exist. Where an Issuing Authority has issued a warrant based on a telephone application and the agency did not comply with the requirement to provide an affidavit, then they may revoke the warrant.

9. Duties to record, report, and destroy

The definitions of a 'restricted record' and 'permitted purpose' are relevant to the obligations within the TIA Act to record, report and destroy. A restricted record means

> a record other than a copy, that was obtained by means of an interception, whether or not in contravention of subsection 7(1), of a communication passing over a telecommunications system, but does not include a record of general computer access intercept information.[39]

---

[38] Section 5 TIA Act.

[39] Section 5 TIA Act.

A permitted purpose is a list of purposes for which an agency can use intercepted communications. These purposes are connected to investigations, functions and activities of agencies.

a) Duty to record and report

The TIA Act provides for significant recording and reporting of information relevant to interception warrants. Sections 80 and 81 TIA Act prescribe what records must be kept by Commonwealth agencies; State and Territory agencies have similar requirements under their own oversight legislation. These provisions detail requirements ranging from retaining copies of warrants and notifications, through to the use by the agency of the information obtained. The Commonwealth Ombudsman and its State and Territory equivalents have the role of inspecting these agency records and reporting annually to the relevant Minister on the outcome of those inspections. The Commonwealth Ombudsman may report on any deficiencies identified that may impact on the integrity of the regime, the details of action taken or proposed remedial action. The Ombudsman may, if there is such a finding, report that in his or her opinion an officer of the agency has contravened a provision of the TIA Act.

There are also significant reporting requirements to the relevant Minister. The Managing Director of a service provider must report annually to the Minister on the number of emergency warrants and Part 2-5 warrants that were executed and revoked. As was noted earlier the Minister provides an annual report to Parliament on the number of warrants issued under Part 2-5, this annual report is based on information obtained from the interception agencies reports to the Minister. The annual report not only reports on statistics but also on the effectiveness of warrants, interception without warrants and mutual assistance requests. The Minister's department also creates a General and a Special Register of warrants which details all warrant information for the purpose of reporting to the Minister for inspection.

b) Duty to destroy

The chief officer of an agency has an obligation to arrange for the destruction of a restricted record where he or she is satisfied that the record is not likely to be required for a permitted purpose of that agency. The chief officer is not to destroy the record until the Minister has inspected the General Register of warrants, referred to earlier. Where the restricted record relates to an interception pursuant to a control order and the chief officer is satisfied that none of the information obtained will assist with the protection of the public from a terrorist act; or preventing the provision of support for, or the facilitation of, a terrorist act; or preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, then the record should be destroyed.

10. Notification duties and remedies

There are no requirements to notify a person that they have been subject to an interception warrant. If a person is charged with an offence, they will become aware of any intercepted material being used in the case during the normal process of police interviews or discovery. It will be a matter for the court to decide a defendant's claim that the interception under warrant was unlawful. As was noted earlier the Commonwealth Ombudsman and State and Territory counterparts undertake inspections to monitor the integrity of the process. If a deficiency in a warrant or the process for collecting the intercept material is found, they can report their findings and recommendations to the relevant Minister.

11. Confidentiality requirements

– *Obligations of telecommunication service providers to maintain secrecy*

Employees of service providers are subject to confidentiality obligations under both the TIA Act and the Telecommunications Act. An employee of a service provider may communicate information about lawfully obtained interception in limited circumstances. These include but are not limited to where it is relevant to their duties in the operation and maintenance of the network, relevant to the supply of services, or to enable the interception or to prevent a terrorist attack.[40] The Act also requires a service provider to protect the confidentiality of information or documents retained under data retention requirements.

Section 276 (1) Telecommunications Act has an established set of principles that require service providers to protect information in their possession, including but not limited to information or documents that relates to the content or substance of a communication and the affairs or personal particulars of another person. A contravention of this section is punishable by imprisonment not exceeding 2 years. The recently introduced technical assistance requirements makes it an offence for a designated communications provider to unlawfully disclose information about a request for assistance under a TAN, TCN, TAR, punishable by imprisonment for 5 years.[41]

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

TIA Act does not use the terminology of traffic or subscriber data, instead disclosures are for information or documents held by service providers. This termi-

---

[40] Section 65A TIA Act.

[41] Section 317ZF Telecommunications Act.

nology is technologically neutral and would include the attribution of dynamic IP addresses if that information is held by a service provider. Under the Telecommunications Act service providers must protect the confidentiality of information that relates to the substance or content of a communication, services supplied and the affairs or personal particulars of persons. The disclosure of information or documents is allowed under law. A distinction is made between existing and prospective information and documents, there are different access regimes which will be discussed below.

a) Collection of traffic and subscriber data

The agencies who may access information or documents (i.e. telecommunications data) are not limited to interception agencies, there are 20 enforcement agencies who can access information or documents from service providers under the TIA Act.[42]

A service provider may voluntarily disclose information or a document to an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty or for the protection of the public revenue. This disclosure envisages the situation where a service provider becomes aware of the information in the course of their business.

An enforcement agency may authorise the disclosure of existing information or documents for the enforcement of the criminal law, a law imposing a pecuniary penalty or protection of the public revenue and for locating missing persons. The disclosure is an internal process and does not require a warrant however the authorised officer must have regard to matters in relation to the privacy of any person or persons. An authorisation may be in writing or electronic. The relevant provisions are:

> Section 178
>
> […]
>
> (2) An authorised officer of an enforcement agency may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation. …
>
> (3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law…

---

[42] The Telecommunications (Interception and Access) Annual Report 2016/2017 stated that 'From 13 October 2015, the definition of enforcement agency was restricted to 20 agencies that also fall under the definition of 'criminal law enforcement agency.' All criminal law enforcement agencies are set out in section 110A TIA Act. These agencies include all interception agencies as well as the Department of Home Affairs, the Australian Securities and Investments Commission and the Australian Competition and Consumer Commission.'

Section 180F

Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate, having regard to the following matters:

(aa) the gravity of any conduct in relation to which the authorisation is sought, including:

(i) the seriousness of any offence in relation to which the authorisation is sought; and

(ii) the seriousness of any pecuniary penalty in relation to which the authorisation is sought; and

(iii) the seriousness of any protection of the public revenue in relation to which the authorisation is sought; and

(iv) whether the authorisation is sought for the purposes of finding a missing person;

(a) the likely relevance and usefulness of the information or documents;

(b) the reason why the disclosure or use concerned is proposed to be authorised.

There is one exception to the agency authorisations noted above found in section 180H TIA Act. It provides if the authorisation relates to

a person who is working in a professional capacity as a journalist; or an employer of such a person; and a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source.[43]

In this situation the agency must make an application to an issuing authority to issue a journalist information warrant. The Issuing authority must be satisfied that

the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source in connection with whom authorisations would be made under the authority of the warrant.

An authorisation for access to prospective information or documents has a higher threshold for access than historical information or documents, being a serious offence or an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years, is limited to 45 days and includes a revocation provision. Section 180 TIA Act is the relevant provision and includes in part:

… Prospective authorisation

(2) An authorised officer of a criminal law-enforcement agency may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force.

Authorisation for access to existing information or documents may also be sought

(3) The authorised officer may, in that authorisation, also authorise the disclosure of specified information or specified documents that came into existence before the time the authorisation comes into force.

---

[43] The Journalist information warrant was introduced as part of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.*

Limits on making the authorisation

(4) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the investigation of:

(a) a serious offence; or

(b) an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years…

b) Data retention

Data retention was introduced into Australian law in 2015. Service Providers are required to retain data specified in the Act for a period of 2 years, but there is no destruction provision so a carrier may retain data for longer periods. The Act specifies what information must be retained as follows:

(1) The following table sets out the kinds of information that a service provider must keep, or cause to be kept, under subsection 187A(1):[44]

Kinds of information to be kept	
Topic	**Description of information**
The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: (i) any name or address information; (ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service, or any related account, service or device.
The source of a communication	Identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.

[44] Section 187AA TIA Act, the Minister may, by legislative instrument, make a declaration modifying (including by adding, omitting or substituting) the data set.

Kinds of information to be kept	
Topic	**Description of information**
The destination of a communication	Identifiers of the account, telecommunications device or relevant service to which the communication: (a) has been sent; or (b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.
The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) the disconnection from the relevant service.
The type of a communication or of a relevant service used in connection with a communication	The following: (a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. (b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. (c) the features of the relevant service that were, or would have been, used by or enabled for the communication. Examples: Call waiting, call forwarding, data volume usage. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).
The location of equipment, or a line, used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: (a) the location of the equipment or line at the start of the communication; (b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.

2. Identification of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

Agencies rely on service providers to assist them with providing the identification of a service or a device, as well as location of mobile terminal devices. It is noteworthy 'the location of equipment, or a line, used in connection with a communication' forms part of the data set under the data retention regime, see above. Australian law has no provisions which address the use of 'IMSI catchers' or 'silent SMS' and there is also no credible reporting on law enforcement's use of the technology. This technology can only be used if it does not interfere with a tele-

communications service or network and does not collect the contents or substance of communications.

D. Access to (Temporarily) Stored Communication Data

1. Online searches with the help of remote forensic software

As noted, Australia has introduced a new CA warrant regime for law enforcement to access data held on computers, including mobile phones. The legislation provides that an agency may apply for a CA warrant for an offence that is punishable by 'a maximum term of imprisonment of 3 years or more or for life'; for recovery orders; for integrity purposes; control orders and for international assistance. A CA warrant must authorise the doing of specified things in relation to a targeted computer. The warrant may include the use of 'any other electronic equipment' and if necessary, with restrictions 'adding, copying, deleting or altering other data.'[45] The SD Act provides for the action taken under a computer access warrant to be concealed.

In addition, the search warrant provisions of the Crimes Act 1914 were recently amended to broaden the powers of examination of computers including access to relevant 'account-based data.' This includes accessing the data on a seized computer or operating that computer to access data, including account-based data held at another place. The supporting documentation to the amendments explained what may constitute account-based data:

> Account-based data in relation to a person includes data associated with an account for an electronic service with end-users that is held by the person. This could be data associated with an email service, a Facebook account, an Instagram account, a Reddit subscription, a Twitter profile, a log-in to a commentary section on a news website or messaging services such as WhatsApp, Signal, and Telegram.[46]

2. Search and seizure of stored communication data

The TIA Act provides a warrant regime for covert access to stored communications that are in the possession of a service provider. It is an offence to access a stored communication without the knowledge of the sender or the receiver of the communication.[47] A stored communication is defined in section 5 TIA Act as:

> a communication that:
>
> (a) is not passing over a telecommunications system; and

---

[45] Section 27E *Surveillance Devices Act 2005.*

[46] Paragraph 774 Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 Explanatory Memorandum, circulated by authority of the Minister for Home Affairs, the Hon Peter Dutton MP.

[47] Section 108 provides a 2-year offence.

(b) is held on equipment that is operated by, and is in the possession of, a carrier; and
(c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

A warrant to access stored communication must be approved by an issuing authority and must satisfy similar thresholds to an interception warrant but there are some clear distinctions.[48] There is a greater number of agencies who can access stored communications including interception agencies, the Australian Border Force, the Australian Securities and Investments Commission and the Australian Competition and Consumer Commission. There is also a different offence threshold to an interception warrant, a criminal law enforcement agency may apply for a warrant for a serious contravention which is defined in section 5E as:

(a) is a serious offence; or
(b) is an offence punishable:
  (i) by imprisonment for a period, or a maximum period, of at least 3 years; or
  (ii) if the offence is committed by an individual – by a fine, or a maximum fine, of at least 180 penalty units; or
  (iii) if the offence cannot be committed by an individual – by a fine, or a maximum fine, of at least 900 penalty units; or
(c) could, if established, render the person committing the contravention liable:
  (i) if the contravention were committed by an individual – to pay a pecuniary penalty of 180 penalty units or more, or to pay an amount that is the monetary equivalent of 180 penalty units or more; or
  (ii) if the contravention cannot be committed by an individual – to pay a pecuniary penalty of 900 penalty units or more, or to pay an amount that is the monetary equivalent of 900 penalty units or more…

An issuing authority must be satisfied that a service provider holds the stored communication, they must also have regard to the level of privacy that will be interfered with, the gravity of the conduct constituting the offence, the extent to which the information will assist in connection with the investigation and whether other methods of investigation have been used or are available. A stored communications warrant does not authorise ongoing access to communications, it provides for a single execution on a service provider, and if there are multiple service providers then one execution on each provider. The warrant remains in force until it is either executed, or for 5 days after it was issued. Stored communications may also be accessed when an interception warrant is executed on a provider.

A precursor to an application for a stored communication warrant is often the execution of a preservation notice upon a service provider. In 2012 a regime to preserve stored communications was introduced as part of Australia's process to accede to the Council of Europe Convention on Cybercrime (Budapest Convention). The preservation notices are used where there is a risk that the stored communica-

[48] It was reported in the 2016/2017 annual report that there were 347 stored communication warrants issued.

tion may be deleted before a warrant is issued. A foreign preservation notice is also available for international requests.[49]

3. Duties to cooperate: production and decryption orders

As noted, in December 2018 new provisions were introduced into the Telecommunications Act to increase the level of technical assistance that a designated communications provider may provide to agencies.[50] The narrative given by Government during the passage of the legislation included that the new powers would assist agencies to manage the challenges of encryption. One of the listed acts or things that can be done is

> removing one or more forms of electronic protection that are or were applied, on or behalf of, the provider where the provider is already capable of removing this protection.[51]

The section 3LA Crimes Act is a provision that enables the police to apply to a magistrate for an order to require a person to assist with accessing evidential information that may be on a computer or data storage device, whether seized or not. This would include disclosing decryption keys, passwords or other security preventing access to the computer or device. It is not necessary for the person to have been involved in the alleged offence. If a person can assist and fails to do so then they may be found guilty of an offence, with a penalty of imprisonment for 5 years or 10 years for a serious offence.

IV. Use of Electronic Communication Data in Judicial Proceedings

1. Use of electronic communication data in the law of criminal procedure

The TIA Act provides that lawfully intercepted communications and stored communications may be used in evidence in an exempt proceeding. The Act defines an exempt proceeding broadly, including but not limited to, criminal prosecutions, bail hearings, police disciplinary and extradition hearings. When introducing evidence in a proceeding, an agency or a carrier may issue an evidentiary certificate which sets out those facts that are considered relevant 'with respect to acts or things done by, or in relation to, employees of the carrier in order to enable a warrant to

---

[49] Australia ratified the Budapest Convention on 29 November 2012.

[50] The legislation is not limited to Australian carriers or carriage service providers but to any provider of communications services and devices in Australia regardless of where they are based.

[51] Section 317E Telecommunications Act.

be executed by either the carrier or the agency'[52] or for an agency's evidentiary certificate, such facts as are considered relevant with respect to 'anything done by an officer or staff member of the agency in connection with the execution of a Part 2 5 warrant…'[53]

A service provider's evidentiary certificate is conclusive evidence of the matters stated in it and an agency certificate is prima facie evidence of the matters stated in the certificate.

2. Inadmissibility of evidence as a consequence of inappropriate collection

The TIA Act does not limit the use of interception or stored communication that is collected in contravention of the Act. Once intercepted material is in evidence it is a matter for the court to determine on the balance of probabilities as to the legality of the collection. In addition, communications that are believed to be intercepted in contravention of the Act may be used to investigate the alleged offence. Finally, where a communication has been intercepted under warrant, but it has been found to be in breach of the Act, the information may be introduced into evidence where the court (or relevant authority) finds that if not for the defect or irregularity, the interception would not have been in contravention of the Act and the irregularity should be disregarded.[54]

3. Use of data outside the main proceedings

The introduction of evidence into a relevant proceeding is not limited to the offence stated in the original application. The TIA Act allows the use of interception material for a permitted purpose which includes a purpose connected with a relevant proceeding. A relevant proceeding is defined in section 6L TIA Act and includes inter alia:

> (1) A reference in this Act, in relation to an agency, or an eligible authority of a State, to a relevant proceeding is, in the case of the Australian Federal Police or a Police Force of a State, a reference to:
>
> (a) a proceeding by way of a prosecution for a prescribed offence that is an offence against a law of the Commonwealth, or of that State, as the case may be; or
>
> […]

This is particularly relevant where an original warrant was for a specific offence and it is determined from the intercepted evidence that the person is committing additional offence/s.

---

[52] Evidentiary certificates are available for interception, stored communications, information or a document and preservation notices.

[53] Section 61 TIA Act.

[54] Sections 75 and 144 TIA Act.

Where an intercepting agency has intercepted material and has identified an offence that was not subject to the warrant but relevant to an investigation of an offence, it may be passed on for investigation and potential prosecution. In 2008, the Victorian Police placed an intercept device on a public telephone in Queensland, under that warrant they intercepted communications which detailed a plot to murder a woman, the intercept material was for a purpose other than the purpose of the warrant. The intercept material was passed to the relevant police and was used to convict two people on conspiracy to murder charges.[55]

Foreign evidence that is to be introduced into an Australian court will be subject to the rules of admissibility in that court, including evidence Acts and court rules. It may be a matter for the foreign jurisdiction to determine the way the evidence will be provided. The Commonwealth Evidence Act provides that evidence may be admitted in paper and electronic forms in Australia's federal courts. The *Foreign Evidence Act 1994* defines how certain evidence obtained under a mutual legal assistance may be used in a proceeding.

4. Challenging the probity of intercepted data

The introduction of evidence into a relevant proceeding is not limited to the offence stated in the original application. Once intercept material is introduced into evidence it no longer attracts the protections of the TIA Act and may be used in evidence in any other matter or used by the media in reporting the case. A defence lawyer will be given the opportunity to listen to or review intercepted material obtained by the police. The defence is entitled to a copy of any of the collected intercepted material and the access to the intercept material will not be limited to the evidence to be introduced.

The jurisdiction's laws of evidence will govern how intercept material is introduced into evidence. If a defendant challenges the validity of intercepted evidence, they will be subject to the evidential law of that court. Expert evidence can be introduced to challenge any aspect of an interception, including voice or technical experts. In addition, a defendant may raise the issue of exculpatory evidence where they believe there is relevant interception information that has not been introduced. It is the judge who has the final decision on the admissibility of evidence or the weight to be given to it. As noted earlier there is very little case law providing guidance on intercepted material used in evidence.

---

[55] *R v Rolls and Sleiman* [2009] VSC 243.

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

1. International Conventions

Australia is party to several international conventions and optional protocols in support of mutual legal assistance in criminal matters. Except for the Budapest Convention these conventions do not specifically address the interception of communications. The relevant treaties and their associated protocols have been implemented in the *Mutual Assistance in Criminal Matters Act 1987* (MACMA Act) or associated regulations.[56]

Australia has given effect to other treaties relevant to mutual legal assistance including the Genocide Convention Act 1949, International Criminal Court Act 2002 and the International War Crimes Tribunals Act 1995.[57]

2. Bilateral treaties

Australia's mutual assistance in criminal matters is administered by cooperative relationships in bilateral and multilateral treaties. Australia also has non-treaty arrangements with countries. Australia has serval bilateral treaties dealing specifically with mutual legal assistance in criminal matters, including with EU member states.

---

[56] Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; Convention on Psychotropic Substances; Single Convention on Narcotic Drugs; Arms Trade Treaty; Convention for the Suppression of the Unlawful Seizure of Aircraft; Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; Convention on Combating Bribery of Foreign Public Officials in International Business Transactions; International Convention for the Suppression of Acts of Nuclear Terrorism; International Convention Against the Taking of Hostages; Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons; Convention on the Physical Protection of Nuclear Material, Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia; Convention on the Safety of United Nations and Associated Personnel; Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation; United Nations Convention against Corruption; Budapest Convention, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime; International Convention for the Suppression of the Financing of Terrorism; International Convention for the Suppression of Terrorist Bombings; United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances; United Nations Convention against Transnational Organised Crime.

[57] Convention on the Prevention and Punishment of the Crime of Genocide Rome Statute of the International Criminal Court UN Security Resolution 827 establishing the International Criminal Tribunal for the former Yugoslavia UN Security Resolution 955 establishing the International Criminal Tribunal for Rwanda.

3. National regulation

The MACMA Act governs international assistance for the collection of evidence in the investigation and prosecution of crime. Australia may make requests to or receive requests from any foreign country. Bilateral treaties assist with the process for accessing evidence. The assistance available in the collection of electronic evidence is through both formal mutual assistance and through police to police or agency to agency arrangements, often the police to police assistance is a precursor to lodging a request.

The MACMA Act provides the framework for international assistance[58] but mainly relies on the specific legislation to provide the rules which govern access. An international assistance request for telecommunications interception is not a purpose for which a warrant may be obtained. However, an international assistance request is available for several other forms of electronic evidence collected under the TIA Act and the SD Act, including telecommunications data, real-time telecommunications data, preservation of the content of a communication, stored communications, surveillance devices, a computer access warrant and access to material that is already in existence including telecommunications interception product.

B. Requirements and Procedure (Including the Handling of Privileged Information)

1. Incoming requests

All requests for international assistance are sent to Australia's central authority within the Attorney-General's Department. The Attorney-General will determine whether to accept or refuse the request. If the request is accepted, the central authority will seek the assistance of the relevant police force to obtain the electronic evidence. The police will apply for the necessary warrant or issue an authorisation to access the evidence.

As noted, Australia does intercept telecommunications on behalf of a foreign country, however where telecommunications interception material that has been lawfully collected and is in the possession of an intercepting agency that may under section 13A MACMA Act and section 68 TIA Act be passed to another country, the information will be passed by the chief officer of an interception agency. Section 68 provides inter alia:

---

[58] Australian legislation uses the terminology of an 'International assistance request.'

Chief officer may communicate information obtained by agency

The chief officer of an agency (in this section called the **originating agency**) may, personally, or by an officer of the originating agency authorised by the chief officer, communicate lawfully intercepted information (other than general computer access intercept information) that was originally obtained by the originating agency or interception warrant information: …

…if the Attorney-General has authorised the provision of the information to a foreign country under subsection 13A(1) of the Mutual Assistance in Criminal Matters Act 1987—to that foreign country, or to the Secretary of the Department administered by that Minister for the purpose of providing the information to that foreign country; …

In addition, section 67 TIA Act provides that an interception agency may communicate lawfully intercepted information to another person for a permitted purpose. This section allows the sharing of intercepted material where there is a joint task force that involves Australia and a foreign country, and the sharing of the information is to progress the Australian agency's permitted purpose.

The TIA Act provides that an agency may apply for a stored communication warrant for an international assistance application, the issuing authority may issue a warrant where they are satisfied that the application relates to an investigation or investigative proceeding of a serious foreign contravention. In issuing the warrant the decision maker must consider the same privacy and proportionality requirements as for domestic applications.[59] The warrant will also be subject to the same time limits as the domestic warrants.

The TIA Act regulates how information collected under a stored communications warrant is communicated. Section 142A(1) TIA Act provides:

(1) If information is obtained through the execution of a warrant issued as a result of an international assistance application, a person may only communicate the information to the entity to which the application relates on the following conditions:

a) that the information will only be used for the purposes for which the entity requested the information;

b) that any document or other thing containing the information will be destroyed when it is no longer required for those purposes;

c) any other condition determined, in writing, by the Attorney-General.

2. Outgoing requests

Australia may apply to a foreign country for telecommunications interception. Such a request will be at the discretion of that country and subject to any conditions which are placed on the material. A law enforcement request for international assistance will be presented to the Attorney-General's Department for approval. If approved the request will be sent to the foreign country for action. The evidence will be sent back to the Department who provides it to the law enforce-

[59] Section 116 TIA Act.

ment agency who made the request. The Department does not have a role in analysing the intercept material, any assessment of the intercepted material is a matter for the receiving agency.

3. Real-time transfer of communication data

Australian law currently does not provide for real-time access to interception so an amendment would be needed to both the TIA and MACMA Acts to facilitate access for a foreign country. The Telecommunications Act and the TIA Act do not place obligations on service providers to assist foreign countries, therefore there are no current provisions to enable direct contact with service providers for assistance. Access to telecommunications data relies on an authorisation of the AFP seeking disclosure under international assistance arrangements. For a foreign country to access information directly from service providers the law would need to be amended to allow for service providers to assist foreign law enforcement in an investigation under the criminal law of a foreign country. In addition, there would need to be a level of checking available to ensure the service provider can be satisfied that processes are in place to ensure that the matter relates to the foreign investigations approved by the central authority. A foreign country would need to establish their own delivery capability for a service provider to send the real-time data, including negotiating a delivery point.

C. Statistics

It is a requirement under the TIA Act to report annually on the number of times lawfully intercepted information or interception warrant information was communicated to a foreign country and the number of stored communications warrants obtained based on a mutual assistance request. The annual report also reports on foreign preservation notices and disclosures of telecommunications data (information or a document) in response to an international assistance request.

In 2016/2017 one authorisation was issued under section 13A for the disclosure of telecommunications interception material, being information that was previously collected by an Australian agency. There were no stored communications warrants issued during the reporting year. 47 authorisations for telecommunications data were made with 18 disclosures to foreign law enforcement agencies in New Zealand, South Africa and Taiwan. 19 foreign preservation notices were issued with no revocations.

List of Abbreviations

AFP	Australian Federal Police
ALR	Australian Law Reports
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Security Intelligence Service
CA warrant	Computer access warrant
CAC	Communications Access Coordinator
FCA	Federal Court of Australia
FCAFC	Federal Court of Australia Full Court
MACMA Act	Mutual Legal Assistance in Criminal Matters Act 1987
SD Act	Surveillance Devices Act 2004
TAN	Technical Assistance Notice
TAR	Technical Assistance Request
TCN	Technical Capability Notice
Telecommunications Act	Telecommunications Act 1997
TIA Act	Telecommunications (Interception and Access) Act 1979
VSC	Supreme Court of Victoria

Austria*

National Rapporteurs:
Christian Bergauer
Diana Bernreiter
Sebastian Gölly
Gabriele Schmölzer

* This report reflects legislation and jurisdiction as of July 2018.

Contents

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Security Services with Powers of Telecommunication Interception

1. National security architecture

According to Article 10 Subsection 1 No. 6 of the Federal Constitutional Law (*Bundes-Verfassungsgesetz*, B-VG)[1] the Federation (therefore the Republic of Austria and not its autonomous provinces, the so-called *Bundesländer*) has the powers of legislation and execution in matters of criminal law (excluding administrative penal law and administrative penal procedure in matters which fall within the autonomous sphere of competence of the provinces) and establishments for the protection of society against criminal or otherwise dangerous elements.[2] Furthermore, the Federation has the powers of legislation and execution in the matters of maintenance of public peace, order and security including the extension of primary assistance in general, but with the exception of local public safety matters (see Article 10 Subsection 1 No. 7 B-VG) and in the matters of organisation and command of the federal police (see Article 10 Subsection 1 No. 14 B-VG) as well as military affairs (see Article 10 Subsection 1 No. 15 B-VG).

Matters of criminal law and of maintenance of public peace, order and security are upheld by a variety of authorities of the Republic of Austria, which are in charge of the prevention and prosecution of crime within the federal state.

Perhaps the most important of these authorities are the public prosecutors, who are – pursuant to the Code of Criminal Procedure (*Strafprozessordnung*, StPO)[3] – competent for criminal prosecution, and the criminal courts, and particularly for deciding whether the accused is guilty or not and – if found guilty – deciding on the sentence.

Additionally, the federal police are an important executing authority. The Austrian federal police are charged with various tasks; these include support of the public

---

[1] BGBl 1/1930 idF BGBl I 22/2018.

[2] As there are few official (or even binding) translations of Austrian laws into English, most of the relevant legal provisions have been translated by the authors themselves. However, there are some translations of Austrian laws provided by the Austrian Federal Chancellery. These are publicly accessible on the internet: see https://www.ris.bka.gv.at/defaultEn.aspx (currentness: 25 April 2019). Where possible these or other translations have been used for this report.

[3] BGBl 631/1975 idF BGBl I 32/2018.

prosecutors in prosecuting crimes. This function is carried out by the so-called criminal police *(Kriminalpolizei)*, i.e., the police that are in charge of criminal investigations. During the preliminary proceedings *(Ermittlungsverfahren)*, the public prosecutors lead the proceedings (Section[4] 20 Subsection 1 StPO; during that stage the public prosecutor is the "master of the proceedings"[5]). They hear evidence and may investigate on their own or order the federal police (in their function as the criminal police) to do so. According to the legal requirements for lawfulness, the investigative measures stipulated in the Code of Criminal Procedure can be divided into different types: some of the investigative measures may be conducted by the criminal police on their own initiative, others require an order by the public prosecutors. The investigative measures requiring an order by the public prosecutors are divided into those the public prosecutors may order on their own without any further authorisation of a court, and those measures that shall be ordered by the public prosecutors on the basis of a court authorisation. According to Section 31 Subsection 1 StPO, a certain (single) judge of the regional court *(Landesgericht)* in whose domicile the competent public prosecutor is located has the power to decide whether the investigative measures in a specific case are legal or not. The particular legal requirements for investigative measures regarding the interception of telecommunications in criminal justice will be outlined later.[6]

Usually, the federal police (in their function as criminal police) start investigating on their own initiative and report to the public prosecutors after finishing their investigations. However, if certain crimes occur, or if investigative measures that may not be carried out by the criminal police on their own are necessary, the criminal police have to report to the public prosecutors in advance, because the public prosecutors are in charge of leading preliminary proceedings and of applying for court authorisations.

In addition to the tasks of the criminal police, the federal police are also competent for the so-called security police *(Sicherheitspolizei)* whose duties concern the maintenance of public peace, order and security. Therefore, the federal police are not only part of the criminal justice system in Austria, but they also have to secure the maintenance of public peace, order and security in advance. It should be emphasised that Austrian policewomen and policemen are generally in charge of both these aforementioned tasks, the criminal police as well as the security police. However, there are many (specialised) police officers whose actual tasks are only criminal investigations. These officers mainly work in the Federal Criminal Police Office (*Bundeskriminalamt*, BKA), which amongst others is in charge of fighting criminal offences within the whole Federation pursuant to the Federal Criminal

---

[4] In Austria, "Section" is actually called "Paragraph" (which is abbreviated with "§").

[5] *Lewisch*, in: Grabenwarter/Schauer (eds.), Introduction to the Law of Austria (2015) 261 (273).

[6] See Chapter III.

Police Office Act (*Bundeskriminalamt-Gesetz*, BKA-G),[7] and the Criminal Police Offices in the Austrian provinces *(Landeskriminalämter)*.

In fulfilling the tasks of the criminal police, the legal basis for the work of the federal police is the Austrian Code of Criminal Procedure. The regulatory framework for their task of maintaining the public peace, order and security is the Austrian Security Police Act (*Sicherheitspolizeigesetz*, SPG).[8]

Apart from the federal police, there is also another (police) authority, which – as an organisational unit of the Directorate General for Public Security *(Generaldirektion für die öffentliche Sicherheit)* – belongs to the Austrian Ministry of the Interior (*Bundesministerium für Inneres*, BM.I): the Federal Office for the Protection of the Constitution and the Fight against Terrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*, BVT). Furthermore, there are corresponding offices in the Austrian provinces, which are established as organisational units of the (Federal) Police Directorates in the Austrian provinces *(Landespolizeidirektionen)*. The legal basis for the work of these authorities is primarily the Austrian Police State Protection Act (*Polizeiliches Staatsschutzgesetz*, PStSG).[9] If the PStSG does not provide any special rules, the general rules of the SPG are applicable on a subsidiary basis.

The relevant military authorities under the legal regime of intelligence or state security law are the Army Intelligence Office (*Heeresnachrichtenamt*, HNaA) and the Counter Intelligence Office (*Abwehramt*, AbwA). These two authorities are organisational units of the Austrian Ministry of Defence. The HNaA is the Austrian foreign intelligence agency, and the AbwA is in charge of counter intelligence measures. The legal basis for their work as intelligence agencies is the Military Warrant Act (*Militärbefugnisgesetz*, MBG),[10] especially Sections 20 to 25.

2. Powers of the interception of electronic communication

As mentioned above, there are various different legal bases for the listed authorities' work within the different legal regimes. Therefore, the particular legal basis provided for the (coercive) interception of electronic communication is summarised for each of the legal regimes separately.

---

7 BGBl I 22/2002 idF BGBl I 118/2016.

8 BGBl 566/1991 idF BGBl I 29/2018.

9 BGBl I 5/2016 idF BGBl I 32/2018.

10 BGBl I 86/2000 idF BGBl I 32/2018.

a) Criminal law

In relation to criminal prosecution, the authorities mentioned above are entitled to intercept electronic communication pursuant to Section 76a StPO and Sections 134 et seqq. StPO. The StPO distinguishes between information on master data and access data (*Auskunft über Stamm- und Zugangsdaten*; Section 76a StPO), information on data of a message transmission (*Auskunft über die Daten einer Nachrichtenübermittlung*; especially Section 134 No. 2 and Section 135 Subsection 2 StPO) and the surveillance of messages (*Überwachung von Nachrichten*; especially Section 134 No. 3 and Section 135 Subsection 3 StPO). Therefore, the StPO provides a legal basis not only for requesting master data, traffic data (as defined in Section 92 Subsection 3 No. 4 of the Telecommunications Act 2003 [*Telekommunikationsgesetz 2003*, TKG 2003][11]), access data (see Section 92 Subsection 3 No. 4a TKG 2003) and location data (see Section 92 Subsection 3 No. 6 TKG 2003) from providers of (tele-)communication services or a service of the information society [see Section 1 Subsection 1 No. 2 of the Notification Act [*Notifikationsgesetz 1999*, NotifG 1999][12]), but it also provides a legal basis for determining the content of messages, which are exchanged or forwarded via a communications network or a service of the information society. The prerequisites for the lawfulness of these investigative measures differ; pursuant to Section 137 Subsection 1 StPO, information on data of a message transmission and the surveillance of messages needs to be ordered by the public prosecutors on the basis of a court authorisation. The details will be provided below.[13]

At present, there is no legal basis for the surveillance of encrypted messages. To rectify this legal loophole (criminals could avoid the "danger" of interception of their electronic communication by using services that encrypt their messages like WhatsApp), a new investigative measure has been introduced: the surveillance of encrypted messages (Section 134 No. 3a and Section 135a StPO). This new investigative measure will enter into force on 1 April 2020. It will cease to be in force on 31 March 2025; within this period of time, an evaluation of this investigative measure is intended. Depending on the outcome of this evaluation, the legislative authorities shall decide on the future of this investigative measure and its legal prerequisites.

b) Preventive law

Besides criminal procedure law, there are also other legal regulations that provide coercive powers for the interception of electronic communication in Austria.

---

[11] BGBl I 70/2003 idF BGBl I 29/2018.

[12] BGBl I 183/1999.

[13] For detailed information on formal prerequisites of interception orders, please see Chapter III.B.6.

Pursuant to Section 53 Subsections 3a and 3b SPG, the authorities *(Sicherheitsbehörden)* may request certain telecommunications data from providers as defined by Section 92 Subsection 3 No. 1 TKG 2003 and other service providers (*Dienstean-bieter*; as defined in Section 3 No. 2 of the Austrian E-Commerce Act [*E-Commerce-Gesetz*, ECG]).[14] On the basis of a number of different prerequisites, the authorities are entitled to get access to data concerning specific electronic communications, e.g., name, address and Internet protocol address (IP-address) of a subscriber (see Section 53 Subsection 3a SPG) or the International Mobile Subscriber Identity and data on the location of a specific mobile device (see Section 53 Subsection 3b SPG). However, the SPG provides no legal basis for the interception of the *content* of electronic communication.[15] As mentioned above, these measures are designed to support the police authorities in preventing crime and in averting dangers.

Pursuant to the PStSG, the BVT and its corresponding offices in the Austrian provinces are also empowered to request certain telecommunications data in order to fulfil the tasks entailed by the PStSG. According to Section 11 Subsection 1 No. 5 PStSG, these authorities may also obtain data under the legal regime of Section 53 Subsection 3a Nos. 1 to 3 and Subsection 3b SPG. Furthermore, Section 11 Subsection 1 No. 7 PStSG provides a legal basis for the request of traffic data, access data and location data. This provision is similar to Section 134 No. 2 StPO. These requests are legal only under certain circumstances and prerequisites (e.g., if they are necessary for the prevention of attacks that endanger the Constitution, etc.). Like the SPG, the PStSG does not provide any legal basis for a legal interception of the *content* of electronic communication.

Neither the SPG, nor the PStSG requires a public prosecutor's order or its confirmation by a judge (or any other court authorisation) for these measures. However, legal protection should have been ensured by legislating a Legal Protection Commissioner of the Ministry of the Interior (*Rechtsschutzbeauftragter beim Bundesminister für Inneres*; see Sections 91a et seqq. SPG). In the cases mentioned in Section 53 Subsection 3a Nos. 2 to 4 and Subsection 3b, the competent authorities have to inform the Legal Protection Commissioner of the Ministry of the Interior about the requests as soon as possible. In the case of Section 11 PStSG, merely to inform the Legal Protection Commissioner of the Ministry of the Interior is not adequate. Pursuant to Section 14 PStSG, the measures listed in Section 11 PStSG are subject to an authorisation of the Legal Protection Commissioner of the Ministry of the Interior; and the competent authorities have to ask for authorisation in advance. In the case of Section 11 Subsection 1 No. 7 PStSG, authorisation is necessary not only from the Legal Protection Commissioner of the Ministry of the In-

---

[14] BGBl I 152/2001 idF BGBl I 34/2015.

[15] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), Wiener Kommentar zur Strafprozessordnung (WK StPO), § 134 mn. 60 and 67 (currentness: April 2016).

terior himself, but also from the Legal Protection Senate (*Rechtsschutzsenat*; see Section 14 Subsection 3 PStSG). The Legal Protection Senate consists of the Legal Protection Commissioner of the Ministry of the Interior and two of his substitutes.

c) Law of intelligence agencies

Apart from the BVT (which is – to a certain degree – also a kind of intelligence agency), there are two military intelligence agencies in Austria, the HNaA and the AbwA. Pursuant to Section 22 Subsection 2a MBG, military organs and authorities in charge of intelligence as well as counter-intelligence measures are empowered to request certain information from operators of public communications services. They may request information on a subscriber's name, address and subscriber number for a certain connection, if they require this information for the performance of their intelligence or counter-intelligence duties. Like the SPG, the MBG does not provide a legal basis for the interception of the *content* of electronic communication; Section 22 Subsection 2a MBG just provides legal provisions that empower the competent authorities to request master data. Therefore, the MBG provides even less legal basis for the interception of electronic communication or data concerning such communication (such as location data) than the SPG or the PStSG.

d) Other law regimes

There are further Austrian legal provisions that provide coercive powers connected to the interception of electronic communication.

First of all, the TKG 2003 provides one legal basis: as communications services are subject to supervision by the regulatory authority (for details see Section 86 Subsection 1 TKG 2003), there are some obligations to provide information (e.g., that relating to the above mentioned legal provisions of the StPO). Moreover, providers of communications services are obliged to provide certain information to administrative authorities: at the written and substantiated request of administrative authorities, they have to provide these authorities with master data (as defined in Section 92 Subsection 3 No. 3 lit. a to e TKG 2003) of subscribers who are suspected of having committed an administrative offence by an act using a public telecommunications network, to the extent that such provision is possible without processing traffic data (Section 90 Subsection 6 TKG 2003).

Pursuant to Section 98 TKG 2003, operators of communications networks or services shall provide information to operators of emergency services, at their request, on master data (as defined in Section 92 Subsection 3 No. 3 lit. a to d TKG 2003) as well as on location data (as defined in Section 92 Subsection 3 No. 6 TKG 2003). Such a request is legal only in the case of an emergency that can be only responded to by providing this information. The emergency service operator shall be responsible for the legal permissibility of the request for information. In

cases where it is not possible to determine a current location, the cell ID of the last communication registered for the communication equipment belonging to the endangered person may be processed. The subscriber concerned shall be informed about such a provision of location data by the provider. The information shall be given at the earliest 48 hours and at the latest 30 days after such provision by sending a short message (SMS) or in writing where it is not possible to send a message. This information shall include the legal basis for the provision of information, the data in question, the date and time of the query and an indication of the body which requested the location data as well as the contact information for that body.

Furthermore, the TKG 2003 provides a legal basis for call tracing. As defined in Section 106 Subsection 1 TKG 2003, call tracing is the process of establishing the identity of a calling line – irrespective of the calling user's will. Call tracing may be requested by a subscriber; it is legal only for the tracing of malicious calls. If requested, the communications service operator shall set up a trace for future calls or have such a trace set up by the communications network operator. The trace may also consist in overriding the elimination of calling line presentation and storage of incoming numbers by the operator. The result of the call trace or of overriding the elimination of calling line presentation shall be stored by the communications service operator and revealed to the subscriber for those calls regarding which the subscriber provides credible evidence that malicious calls were made during the trace.

Besides the TKG 2003, relevant legal provisions can be found in the Law on Financial Crime (*Finanzstrafgesetz*, FinStrG).[16] Pursuant to Section 195 FinStrG, the above-mentioned provisions of the StPO concerning the interception of electronic communication are also applicable for criminal proceedings on financial crimes in which the public prosecutors and criminal courts are competent. In addition to the applicability of these provisions, the FinStrG provides a legal basis for certain requests of finance crime authorities. For the purpose of criminal proceedings on financial crimes, the competent authorities are empowered to request information on a subscriber's name, address and subscriber number from operators of public communications services (see Section 99 Subsection 3 FinStrG). For the prosecution of certain financial crimes, operators of public communications services and other service providers (as defined in Section 3 No. 2 ECG) are obliged to provide information to the competent authorities prosecuting these crimes, at their request, on the name and address of a subscriber to whom a certain IP-address was assigned at a certain time, as well as on the IP-address of a certain message and the date of its transmission, if this is necessary for the above-mentioned request of information on the name and address of a subscriber (for details see Section 99 Subsection 3a FinStrG). The provision of this information is legal only if this data is legally processed at the time of the request.

---

[16] BGBl 129/1985 idF BGBl I 32/2018.

The Austrian customs authorities are also empowered to request certain data from operators of public communications networks and from universal services (see Sections 14 et seqq. TKG 2003) who provide a publicly available telephone service (as defined in Section 3 No. 16 TKG 2003): pursuant to Section 7 Subsection 6 of the Austrian Act to implement Customs Law (*Zollrechts-Durchführungsgesetz*, ZollR-DG),[17] the customs authorities may request information on a subscriber's name, address and subscriber number, if this data is an important requirement for the customs authorities' fulfilling of their tasks according to the ZollR-DG.

3. Responsibility for the technical implementation of interception measures

Generally, investigative measures are carried out by the competent authorities (especially the criminal police that are in charge of supporting the public prosecutors' investigations) themselves. However, there are provisions that empower authorities to request data or information from certain (service) providers and that oblige these providers to supply the necessary technical measures. Therefore, the (service) providers are subject to broad cooperation duties.

Firstly, Section 138 Subsection 2 StPO obliges providers (as defined in Section 92 Subsection 3 No. 1 TKG 2003) and service providers (as defined in Sections 13, 16 and 18 Subsection 2 ECG) to make available information on data of a message transmission (see Section 134 No. 2 and Section 135 Subsection 2 StPO) and to cooperate in the surveillance of messages (see Section 134 No. 3 and Section 135 Subsection 3 StPO). Furthermore, they are obliged to comply with a data preservation order (see Section 134 No. 2b and Section 135 Subsection 2b StPO).

Additionally, there are respective provisions in the TKG 2003. The most important ones for the purposes of this report are the following:

Pursuant to Section 90 Subsection 7 TKG 2003, providers of communications services are obliged to provide the competent (criminal) courts, public prosecutors and criminal police (at their written request) with information on subscribers' master data (as defined in Section 92 Subsection 3 No. 3 TKG 2003) for the purpose of investigation and prosecution of actual suspicions of a criminal offence (see Section 76a StPO). Furthermore, this provision obliges providers of communications services to supply information on data requested according to Sections 53 Subsection 3a No. 1 SPG, Section 99 Subsection 3a FinStrG and Section 11 Subsection 1 No. 5 PStSG. According to Section 90 Subsection 8 TKG 2003, providers of mobile communications networks shall maintain records of the geographical location of the radio cells used to operate their services in order to ensure that a cell ID can be accurately matched to its actual geographical location with an indication of geocoordinates for any point in time within the last six months.

---

[17] BGBl 659/1994 idF BGBl I 120/2016.

Pursuant to Section 94 Subsection 1 TKG 2003, the provider shall be obliged to make available all facilities necessary for monitoring communications and for providing information on data in communications in accordance with the provisions of the StPO, with Section 11 Subsection 1 No. 7 PStSG, with Section 99 Subsection 3a FinStrG as well as those necessary for complying with the duties according to Section 97 Subsection 1a TKG 2003. Furthermore, the provider shall be obliged to cooperate to the required extent in the surveillance of messages and in the provision of information on communications data in accordance with the provisions of the StPO, with Section 11 Subsection 1 No. 7 PStSG and with Section 99 Subsection 3a FinStrG (Section 94 Subsection 2 TKG 2003). Section 94 Subsections 2 and 3 TKG 2003 contain technical specifications concerning the technical facilities necessary for compliance with these cooperation duties and the transmission of the requested data to the competent authorities.

Furthermore, Section 18 Subsection 2 ECG stipulates cooperation duties for access and host providers.

The Ordinance of the Federal Minister for Traffic, Innovation and Technology on the Interception of Telecommunication (*Überwachungsverordnung*, ÜVO)[18] contains more detailed provisions on the precise arrangement of the technical measures that are necessary for the interception of electronic communication. The refund of expenses that such cooperation duties impose on providers is governed by the Ordinance of the Federal Minister for Justice on the Refund of the Providers' Expenses for the Participation in the Information on Data of a Message Transmission, Information on Data Preservation, and the Surveillance of Messages (*Überwachungskostenverordnung*, ÜKVO).[19]

There is, therefore, a broad obligation of cooperation on the above-mentioned service providers.[20]

4. Exchange of results of interceptions of electronic communication between the competent authorities (national and international)

As mentioned above, there are different authorities that are competent and allowed to intercept electronic communication under different legal regimes. The relevant provisions concerning the exchange of results of interceptions of electronic communication between the competent authorities are outlined below. To begin with, it must be pointed out that there must be a differentiation between the exchange of results between two Austrian authorities – which is known as administra-

---

[18] BGBl II 418/2001 idF BGBl II 559/2003.

[19] BGBl II 322/2004 idF BGBl II 133/2012.

[20] For further information on specific cooperation duties of internet providers, please see Chapter III.B.5.

tive assistance *(Amtshilfe)* – and the exchange of results between an Austrian authority and a non-Austrian authority (mutual legal assistance *[Rechtshilfe]*).

a) Exchange of results between the competent authorities within Austria

The probably most important provision on the administrative assistance in matters of criminal law is Section 76 StPO. Pursuant to Section 76 Subsection 1 StPO, the criminal police, the public prosecutors and the criminal courts are empowered to avail themselves of all federal, provincial and municipal authorities and government agencies as well as other bodies and institutions established under public law for the purpose of fulfilling their duties. Furthermore, these authorities, agencies, bodies and institutions are obliged to cooperate as soon as possible (or to immediately inform the criminal police, the public prosecutors and the criminal courts of any circumstances that preclude them from such cooperation); if necessary, these law enforcement authorities are permitted to access records.

According to Section 76 Subsection 2 StPO, the law enforcement authorities' requests for information that concerns a certain person's criminal offences may not be refused due to legal obligations of confidentiality or because the requested information concerns automatically processed personal data – unless these confidentiality obligations explicitly apply for criminal courts or there are prevailing public interests (which need to be cited) that preclude an answer to the request.

Otherwise, the aforementioned law enforcement authorities must not transmit any personal data that was detected due to the provisions of the StPO unless there is a statutory authorisation and its use as evidence in criminal proceedings would also be admissible (Section 76 Subsection 4 StPO). However, if there is an interest in the secrecy of this data which deserves protection (see Section 1 Subsection 1 and Sections 7 et seq. of the Data Protection Act [*Datenschutzgesetz*, DSG][21]) that prevails over the interests of a transmission, the data may not be transmitted. In addition, data that was detected according to Sections 134 et seqq. StPO (therefore, amongst other data that was detected by the interception of electronic communication) may be transmitted to certain authorities only (see Section 76 Subsection 4 No. 1 StPO): it may be transmitted to public prosecutors and criminal courts for the purpose of criminal justice, to police authorities *(Sicherheitsbehörden)* for the purposes of the security police as far as this is necessary to avert serious crimes (as defined in Section 17 SPG) as well as to avert serious danger to life, limb and liberty or substantial assets and property, and, finally, to courts and other authorities for the purpose of the prosecution of disciplinary offences that were committed by

[21] BGBl I 165/1999 idF BGBl I 24/2018.

committing the respective criminal offence or for the purpose of proceedings on civil claims derived from the commitment of the respective criminal offence.[22]

The exchange of results of investigations between the criminal police and the public prosecutors (as well as the criminal courts) in preliminary proceedings which concern the very same proceeding, however, is not based on the legal regime of administrative assistance but on the common task of carrying out the preliminary proceeding (see especially Section 98 StPO).

As Section 76 StPO is probably the most important provision on administrative assistance concerning the exchange of results of the interception of electronic communication, the respective provisions under the other legal regimes will only be briefly outlined.

The probably most relevant provision within the SPG is Section 56. This provision contains prerequisites for the transmission of personal data by police authorities. The transmission is legal, e.g., if the data subject explicitly agrees to it. Furthermore, data may be transmitted to Austrian authorities, if there is a legal basis for the transmission or if the transmission of this data is an important requirement for the recipient to carry out a legal task (see Section 56 Subsection 1 SPG).

Pursuant to Section 12 Subsection 4 PStSG, data may be transmitted to police authorities *(Sicherheitsbehörden)* for the purposes of the security police and criminal justice, and to public prosecutors as well as to ordinary courts for the purposes of criminal justice. Furthermore, this provision allows the transmission of data to constitutional institutions *(verfassungsmäßige Einrichtungen)* pursuant to Section 8 PStSG as well as to other Austrian[23] authorities if the transmission of this data is an important requirement for the recipient to carry out a legal task.

Under the Austrian intelligence law, the probably most important provision regarding the exchange of results and data is Section 25 MBG. Pursuant to this provision's Subsection 1 Nos. 1 to 4, military institutions that are in charge of intelligence and counter-intelligence tasks may transmit data to other Austrian military institutions (as far as these transmissions conduce to the protection of an important public interest), to Austrian authorities if the transmission of these data is an important requirement for the recipient to carry out a legal task and it conduces to the protection of an important public interest, to Austrian military representatives abroad (as far as these transmissions conduce to the protection of an important pub-

---

[22] In addition, Section 76 Subsection 4 StPO states the prerequisites for the transmission of other personal data that was detected according to the (remaining) provisions of the StPO.

[23] In regard to transmissions to non-Austrian authorities (or institutions of the European Union or the United Nations Organisation), Section 12 Subsection 4 PStSG refers to the provisions on the international administrative assistance of police authorities.

lic interest), and to non-Austrian[24] public institutions, international organisations, or transnational institutions[25] if there is a duty under international law to do so, or if the transmission is an important requirement for the performance of intelligence or counter-intelligence tasks. However, the transmission of data is not admissible if there are hints that the transmission would circumvent the protection of editorial confidentiality (*Schutz des Redaktionsgeheimnisses*; as defined in Section 31 of the Media Act *[Mediengesetz]*[26]) or – if the publication of this data endangers the national security or the security of persons[27] (Section 25 Subsection 1a MBG). Furthermore, Section 25 Subsection 2 MBG states reasons for the preclusion of a transmission of data to non-Austrian public institutions, international organisations, or transnational institutions, e.g., if the transmission affects important interests of the Republic of Austria or if it violates duties under international law.

b) Exchange of results between the competent authorities in other countries

Whether the exchange of results of an interception of electronic communication between Austria and other countries is possible depends on the country concerned. There are different legal regimes (e.g., directives of the European Union, international conventions, bilateral treaties, etc.) – each of them stating variable prerequisites. For detailed information on the admissibility of mutual legal assistance concerning the exchange of the results of an interception of electronic communication, please see Chapter IV. below.

B. Statistics on the Interception of Electronic Communication

1. Obligation to collect statistics

Pursuant to Section 93 Subsection 1 SPG, the Austrian federal government is obliged to report on Austria's internal security to the Austrian National Council and the Federal Council. This Security Report *(Sicherheitsbericht)* is compiled by both the Austrian Ministry of the Interior and the Ministry of Justice,[28] and is pub-

---

[24] For reasons of clarity and simplicity, this provision concerning the exchange of information with non-Austrian authorities is outlined together with the administrative assistance under the legal regime of the MBG as the prerequisites are quite similar.

[25] Section 25 Subsection 3 MBG states further requirements for the transmission of data to non-Austrian institutions, international organisations, or transnational institutions, e.g., certain duties concerning the erasure of data.

[26] BGBl 314/1981 idF BGBl I 32/2018.

[27] This restriction, however, does not apply for transmissions to other military institutions.

[28] Since 2017 this Ministry's actual name has been "Ministry of Constitution, Reforms, Deregulation, and Justice" *(Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz)*.

licly accessible on the internet.[29] The Security Reports contain information on committed crimes, the activities in the field of criminal justice, the development of the crime rate, etc. and they provide detailed statistics on these topics. Amongst others, these reports contain statistics on the number of uses of certain investigative measures, e.g., of requests for information on data of a message transmission or of surveillance of messages. For the period from 2010 to 2016,[30] these two statistics are provided below. They show the absolute numbers of interception incidents per year in Austria as a whole (the number of applications for a court authorisation by public prosecutors as well as the number of measures that the court actually authorised). Furthermore, it not only provides total numbers, but also distinguishes between measures concerning the interception of the electronic communication of persons of known identity and those whose identity was unknown. However, not all data concerning the interception of electronic communication or concerning the aforementioned (investigative) measures is available (e.g., these reports do not give data on those measures concerning other law regimes like the MBG).

Furthermore, it has to be noted that – apart from Section 93 SPG which is probably the most important one – there are also other obligations to report statistics to other institutions, e.g., in the Public Prosecutor's Office Act (*Staatsanwaltschaftsgesetz*; StAG).[31] According to Section 10a StAG, the Public Prosecutors' Offices are obliged to report on the number of certain investigative measures that were taken in the Senior Public Prosecutors' Offices over the year. These reports are transmitted to the Minister of Justice who is obliged to send a general report on the number of incidents of these particular investigative measures to e.g., the National Council. This report includes the aforementioned reports of the Public Prosecutor's Offices and of the Legal Protection Commissioner. One of the measures that the Minister will be obliged to report on is the surveillance of encrypted messages (as mentioned above, the provisions on this investigative measure will enter into force in 2020[32]).

---

[29] See https://www.justiz.gv.at/web2013/home/justiz/daten-und-fakten/berichte/sicherheitsberichte~2c94848525f84a630132fdbd2cc85c91.de.html or http://bmi.gv.at/508/start.aspx (currentness: 25 July 2018).

[30] The consulted sources for the statistics below are the Ministry of Justice's parts of the annual Austrian Security Reports for the relevant years, therefore the Sicherheitsbericht 2010, the Sicherheitsbericht 2011, the Sicherheitsbericht 2012, the Sicherheitsbericht 2013, the Sicherheitsbericht 2014, the Sicherheitsbericht 2015, and – the latest one – the Sicherheitsbericht 2016. These reports are available online: see https://www.justiz.gv.at/web2013/home/justiz/daten-und-fakten/berichte/sicherheitsberichte~2c94848525f84a630132fdbd2cc85c91.de.html or http://bmi.gv.at/508/start.aspx (currentness: 25 July 2018).

[31] BGBl 164/1986 idF BGBl I 32/2018.

[32] For details on the surveillance of encrypted messages see below.

2. Current data

a) Information on data of a message transmission (as defined in Section 134 No. 2 StPO)

The following table indicates that the number of court authorisations of a public prosecutor's order concerning information on data of a message transmission was higher in 2016 than it was in 2010. However, its number was smaller than it was in 2013, in 2014, and in 2015.

Year	Number of applications for a court authorisation by a public prosecutor's order (Austria as a whole)			Number of court authorisations of a public prosecutor's order (Austria as a whole)		
	concerning persons of known identity	concerning persons of unknown identity	total	concerning persons of known identity	concerning persons of unknown identity	total
2010	3184	1381	4565	3139	1355	4494
2011	3387	1477	4864	3352	1446	4798
2012	3815	1333	5148	3772	1307	5079
2013	4335	1193	5528	4305	1164	5469
2014	4416	1235	5651	4380	1214	5594
2015	3762	1573	5335	3739	1551	5290
2016	3640	1614	5254	3598	1594	5192

b) Surveillance of messages (as defined in Section 134 No. 3 StPO)

The same holds true for the surveillance of (non-encrypted) messages: the number of incidents was also higher in 2016 than it was in 2010. It is to be noted that there was not just a slight increase, but the number almost doubled. As in the table above, the peak, however, was not in 2016 but earlier (in 2014).

Year	Number of applications for a court authorisation by a public prosecutor's order (Austria as a whole)			Number of court authorisations of a public prosecutor's order (Austria as a whole)		
	concerning persons of known identity	concerning persons of unknown identity	total	concerning persons of known identity	concerning persons of unknown identity	total
2010	1428	209	1637	1416	207	1623
2011	1741	158	1899	1731	156	1887
2012	2088	154	2242	2074	152	2226
2013	2803	213	3016	2787	209	2996
2014	2978	293	3271	2962	290	3252
2015	2182	734	2916	2178	731	2909
2016	2356	674	3030	2341	673	3014

II. Principles of Telecommunication Interception in Constitutional and Criminal Procedural Law

In order to protect a person's electronic communication data and telecommunication data, there are not only legal provisions governing the specific prerequisites for the legitimacy of the interception of electronic communication, but also constitutional safeguards that these specific legal provisions (e.g., the StPO) must be in accordance with. Furthermore, there are some other safeguards that help to protect the secrecy of telecommunication, e.g., criminal law provisions.

As the emphasis of this country report is placed on the criminal procedure law provisions regarding the interception of electronic communication, this Chapter focuses on the safeguards for the interception of electronic communication within this legal regime.

A. Constitutional Safeguards of Telecommunication

In Austria, there are different constitutional safeguards intended to protect electronic communication data. Some of them are part of the "genuine" Austrian law (e.g., the Basic Law on the General Rights of Nationals in the Kingdoms and Länder represented in the Council of the Realm [*Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder*, StGG][33]), others are international law or – at least – are based on international law provisions, e.g., the European Convention on Human Rights (*Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten/ Europäische Menschenrechtskonvention*, EMRK).[34]

Article 10a StGG, Article 8 EMRK, Section 1 DSG and some provisions of the Charter of Fundamental Rights of the European Union (*Charta der Grundrechte der Europäischen Union*, GRC) are outlined below. Furthermore, some more relevant principles are summarised.

1. Article 10a StGG

Article 10a StGG – which has the status of constitutional law – explicitly states the secrecy of telecommunication. Pursuant to Article 10a Subsection 1 StGG, the secrecy of telecommunication *(Fernmeldegeheimnis)* may not be infringed. The Austrian jurisprudence and jurisdiction agree that this provision protects the secrecy of the content of telecommunication, but it does not protect mere master data and location data. However, there is a controversy as to whether it also protects the secrecy of traffic data of telecommunication.[35]

The present constitutional safeguard also provides clear procedural prerequisites for the admissibility of exceptions from the secrecy of telecommunication: pursuant to Article 10a Subsection 2 StGG, exceptions to this provision are admissible only by reason of a judicial warrant in conformity with existent laws. As the wording of Article 10a Subsection 2 StGG is quite distinct, there is no room for exceptions in case of exigent circumstances or similar situations;[36] a judicial warrant (that has to be issued in advance) is always needed. However, although the surveillance of messages shall be ordered by the public prosecutors on the basis of a court authorisation, there are legal academics who doubt that the relevant provisions of the StPO are in accordance with Article 10a Subsection 2 StGG: despite the fact that a judicial warrant is needed, the public prosecutor himself is competent to de-

---

[33] RGBl 142/1867 idF BGBl 684/1988.

[34] BGBl 210/1958 idF BGBl III 144/2016.

[35] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 28 et seq. with further references; *Öhlinger/Eberhard*, Verfassungsrecht[10] (2014) mn. 826.

[36] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 27 with further reference.

cide on his own when the surveillance of a person's messages shall commence or end or whether it shall take place at all. Some legal academics consider this "autonomy" of the public prosecutor to be unconstitutional.[37]

2. Article 8 EMRK

Furthermore, the Austrian provisions regarding the admissibility of the interception of telecommunication have to be in accordance with the constitutional safeguards of the EMRK,[38] especially Article 8, which states the right to respect for private and family life.

Pursuant to Article 8 Subsection 1 EMRK, everyone has the right to respect for his private and family life, his home and his correspondence. The interception of telecommunication/electronic communication is therefore protected by the right to respect for one's private (and family) life as well as by the right to respect for one's correspondence.[39] The right to respect for private and family life as guaranteed by Article 8 EMRK protects not only the secrecy of the content of one's telecommunication, but also the secrecy of traffic data and location data.[40]

Article 8 Subsection 2 EMRK states the prerequisites for the admissibility of exceptions from the right as laid down in Subsection 1: public authorities cannot interfere with the exercise of this right except for such interference that is in accordance with the (national) law and that is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. The legal basis that allows exceptions from the right stated by Article 8 Subsection 1 EMRK needs to be sufficiently accessible and concisely formulated. Furthermore, there has to be some remedy and the interference has to be in accordance with the principle of proportionality.[41]

---

[37] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 26.

[38] The EMRK has constitutional rank in Austria.

[39] According to the European Court of Human Rights' jurisdiction, the term "correspondence" includes not only letters, but also other types of an individual's communications (e.g., telephone conversations): see, e.g., *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 22 with further references. See also *Öhlinger/Eberhard*, Verfassungsrecht[10] mn. 812.

[40] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 22 with further references (especially of relevant jurisdiction of the European Court of Human Rights).

[41] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 23 and 24 both with further references. See also *Öhlinger/Eberhard*, Verfassungsrecht[10] mn. 818 et seqq.

Compared to Article 10a StGG, Article 8 EMRK provides wider protection of the secrecy of telecommunication as it protects not only the content of telecommunication, but also – for example – the secrecy of location data. When it comes to the prerequisites for the admissibility of the interception of telecommunication, Article 8 EMRK is not as restrictive as Article 10a StGG, because the EMRK does not require a judicial warrant for the interception of telecommunication. However, Austrian laws need to conform to the EMRK as well as the StGG. Therefore, exceptions to the secrecy of the content of telecommunications need to conform to the prerequisites of both these constitutional safeguards.

3. Section 1 DSG

One more legal safeguard for electronic communication is Section 1 DSG ("Fundamental right to data protection" [*Grundrecht auf Datenschutz*]). Section 1 DSG is also a constitutional provision. Pursuant to Section 1 Subsection 1 DSG, everyone shall have the right to secrecy of personal data concerning that person, especially with regard to the respect for his or her private and family life, insofar as that person has an interest[42] which deserves such protection. This constitutional provision protects the secrecy of content data, master data, location data and traffic data as long as it concerns an individual.[43]

As Section 1 DSG refers to Article 8 EMRK (especially concerning the [procedural] prerequisites for exceptions from this right – see particularly Section 1 Subsection 2 DSG), further information on the fundamental right to data protection is not necessary.[44]

4. Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union (*Charta der Grundrechte der Europäischen Union*, GRC) also provides constitutional safeguards that may concern the interception of electronic communication. Article 7 GRC (Respect for private and family life) and Article 8 GRC (Protection of personal data) are particularly relevant. However, the provisions of the GRC are only applicable for Member States when implementing Union law. Furthermore, the content of these provisions essentially accords with Article 8 EMRK.[45] There is thus no need to

---

[42] According to that provision, such an interest is precluded if data cannot be subject to the right to secrecy due to the data's general availability or because it cannot be traced back to the data subject.

[43] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 30 with further references.

[44] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 30. See also *Öhlinger/Eberhard*, Verfassungsrecht[10] mn. 827 et seqq.

[45] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 21.

provide further information on these provisions as there are no additional constitutional prerequisites for the admissibility of the interception of electronic communication that originates from these provisions of the GRC.

5. Principles of legality

As mentioned above, legal provisions that interfere with fundamental rights – e.g., concerning the admissibility of the interception of electronic communication – need to be in accordance with the principle of proportionality.

Furthermore, the Constitution contains the principle of legality *(Legalitätsprinzip)*. Pursuant to Article 18 Subsection 1 B-VG, public administration in its entirety shall be based on law. Therefore, a legal basis for every action of the public administration is needed. Additionally, the laws need to be determined and intelligible.[46]

According to the wording of Article 18 Subsection 1 B-VG, the principle of legality only applies to public administration, but not to the courts of justice (*ordentliche Gerichte*, e.g., the criminal courts). However, in fact the principle of legality also applies to the courts of justice, deriving (at the most it can be derived from Article 89 Subsection 1 B-VG).[47] Thus, the courts of justice also require a legal basis for its activities. Laws (especially those concerning criminal matters – for instance those providing a legal basis for the admissibility of the interception of electronic communication) also need to be determined and intelligible.[48]

B. Specific Non-Constitutional Protection for Electronic Communication and for Computer-Stored Data

Apart from the constitutional safeguards mentioned above, there are also non-constitutional legal provisions intended to protect the (secrecy of) electronic communication. First of all, protection is provided by the legal provisions concerning the admissibility of the interception of electronic communication themselves (see above;[49] e.g., Sections 134 et seqq. StPO). They provide explicit prerequisites

---

[46] *Berka*, Verfassungsrecht[6] (2016) mn. 492 and 500 et seqq. See also *Grabenwarter/Holoubek*, Verfassungsrecht – Allgemeines Verwaltungsrecht[2] (2014) mn. 763 et seqq.; *Hinterhofer/Oshidari*, System des österreichischen Strafverfahrens (2017) mn. 2.52 et seqq.; *Öhlinger/Eberhard*, Verfassungsrecht[10] mn. 344 et seq. And 598 et seqq.

[47] *Berka*, Verfassungsrecht[6] mn. 494; *Hinterhofer/Oshidari*, System mn. 2.52; *Öhlinger/Eberhard*, Verfassungsrecht[10] mn. 639; *Wiederin*, in: Fuchs/Ratz (eds.), WK StPO § 5 mn. 13 with further references (currentness: October 2013). For detailed information see *Lewisch*, Verfassung und Strafrecht (1993) 112 et seqq. (especially 119 et seqq.) with further references.

[48] *Berka*, Verfassungsrecht[6] mn. 509. See also *Öhlinger/Eberhard*, Verfassungsrecht[10] mn. 601 et seqq.

[49] These provisions have been outlined above and will be explained more detailed below (see Chapter III.).

that rule whether an interception of electronic communication (in a certain case or under certain circumstances) is legal or not. As these provisions have been outlined above and will be explained in more detail below, these will not be further discussed here.

However, there are further provisions concerning the application of those provisions. Moreover, the unauthorised interception of another person's electronic communication is penalised under some provisions of the Austrian Criminal Code (*Strafgesetzbuch*, StGB).[50] The provisions concerning the principles above and the respective criminal offences are outlined below.

The question whether evidence that was collected by an inadmissible interception of electronic communication is admissible and may be used in court proceedings will be answered in detail below.[51]

1. The principles of proportionality and legality within the StPO (and the SPG)

Pursuant to Section 5 Subsection 1 StPO, the criminal police, public prosecutors and the criminal courts have to exercise their powers and investigate (i.e., collect evidence) in a way that does not interfere with the rights of a person if there is no appropriate legal basis for this interference. Furthermore, such interference is legal only if it is necessary for the performance of their tasks; the criminal police, public prosecutors and the criminal courts have to choose the option from amongst all the productive investigative measures and means of coercion available to them that has the least impact on the rights of the person concerned (see Section 5 Subsection 2 StPO).[52]

Moreover, Section 5 Subsection 1 StPO states that every interference in a person's rights needs to be proportionate to the seriousness of the offence (the person is charged with), the level of suspicion and its desired success.[53]

The interception of electronic communication that is based on the legal regime of the criminal law (respectively the StPO) therefore needs to be in accordance not only with the specific legal provisions concerning the admissibility of the interception of electronic communication, but also with these important principles generally applicable during criminal prosecutions.

For the legal regime of the SPG, the principle of proportionality is stated in Section 29.

---

[50] BGBl 60/1974 idF BGBl I 117/2017.

[51] See Chapter III.E.

[52] *Hinterhofer/Oshidari*, System mn. 2.52.

[53] See also *Hinterhofer/Oshidari*, System mn. 2.59.

2. Criminal offences that could be carried out by intercepting one's electronic communication

An inadmissible interception of another person's electronic communication may be punishable under the criminal offences regarding such acts.

Section 119 StGB[54] penalises a breach of telecommunications confidentiality *(Verletzung des Telekommunikationsgeheimnisses)*.[55] According to this provision, any person who uses a device that is connected to a telecommunications or computer system (as defined in Section 74 Subsection 1 No. 8 StGB[56]) or that has otherwise been prepared to receive communication for the purpose of acquiring knowledge for himself, herself or for another unauthorised person of a message transmitted by way of telecommunication or through a computer system and that is not intended for the person, is liable to imprisonment for up to six months or a fine not exceeding 360 penalty units[57].[58] This provision therefore protects the content of any message that is transmitted via telecommunications or through a computer system. However, there is no criminal liability if the interception of telecommunication/electronic communication is justified by a provision, such as Section 134 No. 3 and Section 135 Subsection 3 StPO.[59] Furthermore, criminal liability under Section 120 Subsection 2a StGB (Improper use of audio recording and listening devices; *Missbrauch von Aufnahme- oder Abhörgeräten*) is possible: any person who records, makes available to another unauthorised person, or publishes a message transmitted by way of telecommunication and not intended for the person, for the purpose of acquiring knowledge for himself, herself, or for another unauthorised person, is liable to imprisonment for up to three months or a fine not exceeding 180 penalty units, unless the offence is punishable with a higher penalty under any other offence (especially with Sections 118 et seqq. StGB).[60]

---

[54] The wording of the criminal offences illustrated in this Chapter originates from the translation of the Austrian Strafgesetzbuch in *Schloenhardt/Höpfel* (eds.), Strafgesetzbuch. Austrian Criminal Code (2016).

[55] For details concerning this offence see *Bergauer*, Das materielle Computerstrafrecht (2016) 154 et seqq. with further references.

[56] This term involves not only "classical" computers, but also laptops/notebooks, servers, mobile phones, tablet PCs and so on: see *Birklbauer/Hilf/Tipold*, Strafrecht Besonderer Teil I[4] (2017) 269 with further references (concerning the justification see p. 276).

[57] According to Section 19 StGB, fines are imposed in per diem penalty units. The amount of one (per diem) penalty unit is determined for each person individually (considering the personal circumstances and financial capacity of the individual). The penalty unit is to be set at a minimum of 4 Euro and a maximum of 5000 Euro. (The wording of this translation of Section 19 StGB also originates from *Schloenhardt/Höpfel* [eds.], Strafgesetzbuch. Austrian Criminal Code, 31.)

[58] *Schloenhardt/Höpfel* (eds.), Strafgesetzbuch. Austrian Criminal Code, 163.

[59] See also *Bergauer*, Computerstrafrecht, 154 et seqq. with further references; *Birklbauer/Hilf/Tipold*, Strafrecht BT I[4] 273 et seqq. with further references (concerning the justification see p. 276).

[60] *Schloenhardt/Höpfel* (eds.), Strafgesetzbuch. Austrian Criminal Code, 165. For details see *Bergauer*, Computerstrafrecht, 216 et seqq. with further references.

Moreover, there may be criminal liability according to Section 119a StGB (Improper interception of data; *Missbräuchliches Abfangen von Daten*). Pursuant to this provision, any person who uses a device that is connected to a computer system or that has otherwise been prepared to receive communication, or who collects the electromagnetic irradiation of a computer for the purpose of acquiring knowledge for himself, herself or for another unauthorised person of data that have been transmitted by a computer system and that are not intended for the person and have the purpose to obtain a financial or other material benefit for himself, herself, or another or causing a detriment to another by using the data himself or herself, by making them available to another, or by publishing them, is liable to imprisonment for up to six months or a fine not exceeding 360 penalty units, unless the offence is punishable under Section 119 StGB.[61] As defined in Section 74 Subsection 2 StGB, data means not only personal data, but also non-personal data and programs. Therefore, this term has a much broader meaning than "message" (cf. Section 119 StGB). Again, the justification of a legal power that declares such an interception admissible averts any criminal liability.[62]

In addition, gaining access to computer-stored data inadmissibly may be a criminal offence under Section 118a StGB (Unlawful use of a computer system; *Widerrechtlicher Zugriff auf ein Computersystem*). Pursuant to this provision, any person who gains access to a computer system, which the person is not authorised to use or not authorised to use by himself or herself, or who partially gains access to a such a computer system by overcoming specific security settings for the purpose of either acquiring knowledge for himself, herself or another unauthorised person of personal information, knowledge of which violates confidentiality interests worthy of protection, or causing a detriment to another by using the information to which the person gained access that is saved in the computer system and that is not for his or her attention or by using the computer system, is liable to imprisonment for up to six months or a fine not exceeding 360 penalty units. If the offence involves a computer system that is a significant component of critical infrastructure as defined in Section 74 Subsection 1 No. 11 StGB, the perpetrator is liable to imprisonment for up to two years (Section 118a Subsection 2 StGB). Furthermore, if the offence is committed in connection with a criminal association, the perpetrator is liable to imprisonment for up to two years; but if the offence involves a computer system that is a significant component of critical infrastructure and the offence is committed in connection with a criminal association, the perpetrator is liable to imprisonment for up to three years.[63] Such "specific security settings" are for instance passwords or fingerprint identification; if there is no such "specific security setting,"

---

[61] *Schloenhardt/Höpfel* (eds.), Strafgesetzbuch. Austrian Criminal Code, 164.

[62] See also *Bergauer*, Computerstrafrecht, 199 et seqq. with further (more detailed) references; *Birklbauer/Hilf/Tipold*, Strafrecht BT I[4], 273 et seqq. with further references (concerning the justification see p. 276).

[63] *Schloenhardt/Höpfel* (eds.), Strafgesetzbuch. Austrian Criminal Code, 162.

criminal liability is averted – even if the unsecured computer system is stored in a locked room.[64] Criminal liability of a person who is in charge of criminal investigations or of the prosecution of crime is also averted if the interception (and use) is justified by a power such as provided by Sections 110 et seqq. StPO.[65]

According to Section 118a Subsection 3, Section 119 Subsection 2, Section 119a Subsection 2 and Section 120 Subsection 3 StGB, the perpetrators may not be prosecuted unless the victim has authorised the prosecution (therefore, these offences are so-called *Ermächtigungsdelikte*).

Furthermore, criminal liability may be attached to a person who misuses their authority/power as a government official (as defined in Section 74 Subsection 1 No. 4 StGB). Firstly, an inadmissible interception ordered or carried out by a government official may be qualified as a misuse of official authority (*Missbrauch der Amtsgewalt*; Section 302 StGB). Pursuant to this provision, any person being a government official, who knowingly misuses his or her authority to execute official duties as an organ and in the name of the Republic of Austria, a State, a municipalities association, a municipality, or another entity under public law, intending thereby to violate the rights of another, is liable to imprisonment for six months to five years. If the offence is committed in the course of official duties involving a foreign power or a supranational or intergovernmental entity, or the offence causes damages exceeding 50,000 Euro, the perpetrator is liable to imprisonment for one to ten years.[66]

According to Section 313 StGB, the maximum penalty for the criminal offences that have been mentioned above (except for Section 302 StGB) – either imprisonment or fine – may be exceeded by more than half, if the intentional offence is committed by a government official who is abusing an opportunity provided to him or her in his or her official capacity. However, the maximum term of imprisonment may not exceed twenty years.[67] Therefore, a government official who breaches for instance the telecommunications confidentiality as defined in Section 119 Subsection 1 StGB is liable to imprisonment for up to nine months or a fine not exceeding 540 penalty units (Section 119 Subsection 1 in connection with Section 313 StGB).

In addition, the TKG 2003 contains further provisions that state criminal offences. Pursuant to Section 108 Subsection 1 TKG 2003, certain violations of the rights of users *(Verletzung von Rechten der Benützer)* shall be punished by the (criminal) court with a prison sentence of up to three months or a fine of up to 180 penalty units, unless the offence is punishable with a more severe penalty under any other offence. According to this provision, any person as defined in Section 93 Subsec-

---

64 *Birklbauer/Hilf/Tipold*, Strafrecht BT I[4], 270 et seq. with further references.

65 For details see *Bergauer*, Computerstrafrecht, 74 et seqq. with further references.

66 *Schloenhardt/Höpfel* (eds.), Strafgesetzbuch. Austrian Criminal Code, 372.

67 *Schloenhardt/Höpfel* (eds.), Strafgesetzbuch. Austrian Criminal Code, 386.

tion 2 TKG 2003[68] who either – without authorisation – discloses the fact or the contents of the telecommunications traffic of specific persons to an unauthorised person or gives such a person the opportunity to perceive facts himself that are subject to the obligation to maintain secrecy, or falsifies, incorrectly relates, modifies, suppresses or incorrectly conveys a communication or withholds it from the intended recipient without authorisation, is liable to the above-mentioned penalties.

3. Administrative penalties

Apart from a liability for the criminal offences outlined above, inadmissible interceptions of electronic communication may also result in administrative penalties. Administrative offences concerning – amongst others – inadmissible interceptions of electronic communication are stated in Section 109 TKG 2003. According to this provision, the authorities may impose fines of up to 58,000 Euro for certain violations of the laws.

The most important administrative offences concerning the interception of electronic communication are outlined below.

Pursuant to Section 109 Subsection 3 No. 21 TKG 2003, any person who violates Section 99 Subsection 5 TKG 2003 by providing information on traffic data or processing traffic data for information purposes, shall be guilty of an administrative offence and shall be punished by a fine of up to 37,000 Euro.

Furthermore, there are administrative offences concerning violations of the laws in conjunction with the cooperation of providers with public authorities such as police authorities or public prosecutors. According to Section 109 Subsection 3 No. 22 TKG 2003, any person who violates Section 94 Subsection 2 TKG 2003 by transmitting traffic data, location data and master data which requires the processing of traffic data under the provisions of the StPO, the SPG,the PStSG or the FinStrG without encryption (for details see Section 94 Subsection 2 TKG 2003), shall be guilty of an administrative offence and shall be punished by a fine of up to 37,000 Euro. Any person who violates Section 99 Subsection 2 No. 4 TKG 2003 by erasing data that should be saved due to a preservation order by the public prosecutor (Section 135 Subsection 2b StPO; for details see below) shall be guilty of an administrative offence and shall be punished in the same way (Section 109 Subsection 3 No. 23 TKG 2003). Additionally, any person who violates Section 90, Section 94 Subsection 2, or Section 98 TKG 2003 by not providing the authorities with the requisite data, by not cooperating to the required extent in the surveillance of messages and in the provision of information on data of a message transmission, or by not providing information to operators of emergency services with master data

---

[68] Such persons are the operators of a public communications network or service and all persons who are involved in the operator's activities. Pursuant to this provision, these persons shall observe confidentiality of the communications.

as well as location data or by not informing the subscriber about such a provision, shall be guilty of administrative offence and shall be punished by a fine of up to 37,000 Euro (Section 109 Subsection 3 Nos. 13, 14, and 17 TKG 2003).

According to Section 109 Subsection 6 TKG 2003, these administrative offences shall not exist if the punishable act is a criminal offence that falls within the jurisdiction of the (ordinary criminal) courts or is subject to a more severe penalty according to other administrative penal provisions.

C. Principles for the Definition of Coercive Powers in Criminal Procedural Law

Pursuant to Section 5 Subsection 1 StPO, there must not be any interference in the rights of a person without an explicit legal provision allowing such an interference.[69] Therefore, every investigative measure that interferes in the rights of a person needs a legal basis. As mentioned above, there are also constitutional safeguards on the need for a legal provision – e.g., Article 18 B-VG (at the most in conjunction with Article 89 B-VG) or fundamental rights that state certain conditions for allowing an interference with them (such as Article 10a StGG or Article 8 EMRK).

These provisions outline the principles that coercive powers in criminal procedural law (like the interception of electronic communication) must accord with, e.g., the principles of legality and proportionality.

Therefore, criminal investigative measures like the interception of electronic communication need a precisely defined legal basis. This legal basis can be found in Sections 134 et seqq. StPO that will be explained in detail later.[70]

The prohibition of analogy does not apply for criminal procedural law, but only for substantive criminal law (see Section 1 StGB). Since Section 5 StPO entered into force in 2008, the Austrian jurisprudence and legal academics, however, have broadly agreed that analogies are also prohibited in criminal procedural law if such an analogous application of legal provisions interferes in a person's (fundamental) rights.[71] To a certain extent, the need for an explicit (in terms of *not only by an*

---

[69] See also *Kroschl*, in: Schmölzer/Mühlbacher (eds.), StPO Strafprozessordnung Praktikerkommentar [1.02] § 5 mn. 5 with further references (currentness: March 2013); *Hinterhofer/Oshidari*, System mn. 2.52 et seqq.

[70] See Chapter III.

[71] See, e.g. *Hinterhofer/Oshidari*, System mn. 2.58; *Kroschl*, in: Schmölzer/Mühlbacher (eds.), StPO[I.02] § 5 mn. 5 with further references; *Seiler*, Strafprozessrecht[16] (2017) mn. 10 with further references; OGH 15 Os 180/13d = EvBl 2015/28 = JBl 2015, 735 (*Reindl-Krauskopf*) = SSt 2014/42 with further references. See also *Wiederin*, in: Fuchs/Ratz (eds.), WK StPO § 5 mn. 53 and 69 et seq. with further references. According to *Wiederin*

analogous application of a similar provision) legal basis for such interferences can also be derived from the wording of the respective fundamental rights,[72] e.g., Article 10a StGG ("in conformity with existent laws"; *in Gemäßheit bestehender Gesetze*) or Article 8 Subsection 2 EMRK ("in accordance with the law"). However, an analogous application of legal provisions is generally possible where they are in favour of the suspect/accused.[73]

As a result, an analogous application of coercive powers (such as the interception of electronic communication) would not be legal under Austrian criminal procedural law. Therefore, the permitted types of interception of electronic communication – and the respective prerequisites for their admissibility – are comprehensively contained in the Austrian StPO (see especially Sections 134 et seqq. StPO; for details see below).

Finally, it has to be noted that both the legal provisions about (the admissibility of) the interception of electronic communication as well as the *application of these provisions,* must conform with Section 5 StPO (and the respective constitutional safeguards). Thus, each decision about the admissibility of such a measure in every case (and its enforcement) has to be in accordance with Section 5 StPO and therefore needs to be substantiated and proportionate.[74]

III. Authority to Access Telecommunication Data in the Law of Criminal Procedure

A. Overview

1. Commencement and ending of criminal or investigation proceedings

The Code of Criminal Procedure (StPO) lays down the procedures for the investigation of criminal offences, the prosecution of suspected persons and related decisions. Criminal proceedings begin as soon as the criminal police (i.e., the police responsible for criminal investigations) or public prosecutor begin to investigate an initial suspicion (*Anfangsverdacht*; Section 1 Subsection 2 StPO). In accordance with Section 1 Subsection 2 StPO, an initial suspicion arises when it can be as-

(in: Fuchs/Ratz [eds.], WK StPO § 5 mn. 54), however, there is a general prohibition of analogy *in malam partem* also in criminal procedural law.

[72] *Wiederin*, in: Fuchs/Ratz (eds.), WK StPO § 5 mn. 18.

[73] See especially *Wiederin*, in: Fuchs/Ratz (eds.), WK StPO § 5 mn. 54; *Hinterhofer/Oshidari*, System mn. 2.58. According to *Kroschl* (in: Schmölzer/Mühlbacher [eds.], StPO[1.02] § 5 mn. 5], the analogous application of criminal procedural provisions is also possible if it is not in favour of the suspect/accused – as far as his/her fundamental respective individual rights *(subjektive Rechte)* are not affected.

[74] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 25.

sumed, due to certain indications, that a crime has been committed. Criminal proceedings end by the public prosecutor or court closing or abandoning the prosecution (Section 1 Subsection 2 last sentence StPO).

2. Investigating procedure and using types of information accessible to the public or internal sources

Regarding Section 91 Subsection 1 StPO, the investigating procedure serves to clarify facts and suspicions by investigation. Indeed, the prosecutor may decide on charges, withdrawal from the prosecution or cessation of proceedings. In the case of indictment, the prosecutor may decide to conduct the main proceedings. Investigation means any activity carried out by the criminal police, public prosecutor or court, which is used to obtain, secure, evaluate or process information to clarify the suspicion of a crime. The investigation is performed in accordance with the process stipulated in this act either as an inquiry or as evidence. The mere use of information which is publicly accessible or only intended for internal use by public authorities, as well as clarifying inquiries as to whether an initial suspicion exists, do not constitute an investigation in this sense (Section 91 Subsection 2 StPO).

3. Principles of legality and proportionality

The investigative authorities may only intervene in the rights of persons by exercising their powers so far as legally provided (Section 5 Subsection 2 StPO). Every intervention must be proportionate to the seriousness of the offence, level of suspicion and the desired success. Among several investigative actions and coercive measures, the criminal police, public prosecutor and court, must opt for those which have the least impact on the rights of the persons concerned. Powers granted by law must be exercised at every stage of the proceedings. This must be in a manner which avoids unnecessary attention, respects the dignity of the persons and safeguards both their rights and legitimate interests (Section 5 Subsection 2 StPO).

4. The processing of personal data

With regards to the processing of personal data, the criminal police, public prosecutor and court have to respect the principles of legality and proportionality (Section 5 StPO). They have to protect the legitimate interests of a person's secrecy and give priority to the treatment of confidential data. When processing sensitive personal data or data relevant to criminal law, the criminal police, public prosecutor and court have to make appropriate measures for protecting the interests of a person's secrecy. Unless otherwise stated, personal data is processed under the provisions of the data protection act.

5. Information on master and access data

At the request of the criminal police, public prosecutor or court, providers of communication services have to provide authorities with information on a subscriber's master data (*Stammdaten*; as defined in Section 92 Subsection 3 TKG 2003) for clarifying a suspected criminal offence (Section 76a Subsection 1 StPO in connection with Section 90 Subsection 7 TKG 2003).

The same applies, under Section 76a Subsection 2 StPO, to the information related to specific access data (*Zugangsdaten*; as defined in Section 92 Subsection 4a TKG 2003) stored on technical equipment. However, this can only be requested by the public prosecutor.

6. Seizure and confiscation

The provisions on seizure (*Sicherstellung*; as defined in Section 109 No. 1 StPO) and confiscation (*Beschlagnahme*; Section 109 No. 2 StPO) are covered by sections 110 to 115. In this context the provision of Section 111 StPO is to be mentioned, particularly regarding traffic information stored by data carriers.

It is permitted to search a publicly inaccessible piece of land, a room, vehicle, container, flat or location that is protected by domestic authority. This encompasses a search of the objects located therein. The provisions relating to the search of premises and objects apply (*Durchsuchung von Orten and Gegenständen*; as defined in Section 117 No. 2 StPO). Where appropriate, this incorporates the search of a person (*Durchsuchung einer Person*; Section 117 No. 3 StPO) (Sections 119 et seqq. StPO).

7. Information on data of a message transmission

The term "information on data of a message transmission" *(Auskunft über Daten einer Nachrichtenübermittlung)* is defined in Section 134 No. 2 StPO. It describes information on traffic data (as defined in Section 92 Subsection 3 No. 4 TKG 2003), access data (Section 92 Subsection 3 No. 4a TKG 2003) and location data (*Standortdaten*; Section 92 Subsection 3 No. 6 TKG 2003). Such data can be obtained from a telecommunications service, or a service of the information society (Section 1 Subsection 1 No. 2 NotifG 1999). Relevant information is given under the Sections 135 Subsection 2, 137 et seqq., 147 StPO.

8. Surveillance of messages

The surveillance of messages *(Überwachung von Nachrichten)* is defined in Section 134 No. 3 StPO as determination of the contents of messages which are exchanged or forwarded via a communications network or a service of the information society. The specific regulations are to be found under the Section 135 Subsection 3, Sections 137 et seqq., 147 StPO.

9. Surveillance of encrypted messages

To close the gaps in law enforcement resulting from technical progress, a new investigative measure for the surveillance of encrypted messages *(Überwachung verschlüsselter Nachrichten)* with a comprehensive legal protection concept has been introduced. This measure may be implemented only in a specific criminal procedure based on a concrete suspicion of offences, and not for the surveillance of an unspecified number of persons. A court authorisation, based on a reasoned order by the public prosecutor, is always required.

10. Data preservation (quick-freeze)

Data preservation, also known as "quick freeze" *(Anlassdatenspeicherung)*, is only applied from the moment an initial suspicion of specific offences arises, based on a preservation order from the public prosecutor which obliges communication service providers to save traffic, access and location data for up to 12 months.

B. Interception of Content Data[75]

1. Statutory empowerment

Since 1 June 2018,[76] Section 134 No. 3 StPO has defined interception of content under "surveillance of messages" as the determination of the contents of messages, which are sent, transmitted or received by a natural person via a communications network (Section 3 No. 11 TKG 2003) or a service of the information society (Section 1 Subsection 1 No. 2 NotifG). The aim of this reformulation was to create a separate and meaningful definition for surveillance of messages,[77] i.e., a definition that was independent from the respective message definitions in the TKG 2003 (Section 92 Subsection 3 No. 7 TKG 2003) and in the Austrian Criminal Code (Section 119 StGB); in short, a clear and transparent definition of message specific to the StPO,[78] and a definition that makes it clear that the surveillance of messages is not limited to a finite number of persons involved.[79]

---

[75] Please note that the report also contains information on provisions that will be in force from 1 April 2020 to 31 March 2025, particularly the provisions concerning the surveillance of encrypted messages. For details see *Gölly*, jusIT 2018, 83 (88 et seq.).

[76] Law amending the Code of Criminal Procedure 2018 *(Strafprozessrechtsänderungsgesetz 2018)*, BGBl I 27/2018.

[77] ErlRV 17 BlgNR XXVI. GP, 1.

[78] For a comprehensive discussion of the reformulation see *Gölly*, Gesetzgebungsmonitor zum sog. „Sicherheitspaket": Regierungsvorlage für ein Strafprozessrechtsänderungsgesetz 2018 und Regierungsvorlage für Änderungen im Sicherheitspolizeigesetz in der Straßenverkehrsordnung 1960 und im Telekommunikationsgesetz 2003 – Teil 1, jusIT 2018, 46 et seq.

[79] ErlRV 17 BlgNR XXVI. GP, 8.

Section 135 Subsection 3 StPO outlines the substantive requirements for a lawful surveillance of messages (see below Chapter III.B.7.).

2. Scope of application

The legal definition in Section 134 No. 3 StPO continues to cover human thought content (conventional phone calls, SMS or MMS, voice messages, video messages, e-mails, etc.), but also information that natural persons send, transmit or receive via communication networks (Section 3 No. 11 TKG 2003) or information society services (Section 1 Subsection 1 No. 2 NotifG 1999), i.e., it also includes communications in a technical sense, e.g., when someone opens a website, surfs the internet, or performs unencrypted transfers to a cloud service[80]. However, the definition only includes types of communications that involve at least one natural person, thereby making it clear that this is not an instrument for the surveillance of autonomous communications, e.g., between two machines (M2M communication).[81]

Section 3 No. 11 TKG 2003 defines communications networks as transmission systems and their accessory equipment – including inactive network elements – which permit the electronic transmission of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed and mobile terrestrial networks, electricity cable systems and audio, television and cable broadcasting networks.

As the new legal definition in Section 134 No. 3 StPO solely refers to the above outlined provision of the Telecommunications Act, but does not adopt the concept of message defined therein (Section 92 Subsection 3 No. 7 TKG 2003), there is no longer an implicit limitation to public communications services (Section 3 Subsection 9 TKG 2003). In the absence of an explicit publicity criterion in the StPO concept of message and against the background that this aspect is not mentioned in the legislative texts, one can assume that the legislator either deliberately extended the surveillance of messages to non-public communications (e.g., e-mail traffic on a local network with no connection to a public network) or that it was an error in the legislative process. It will be difficult to interpret the new provision restrictively by carrying out a teleological reduction to read it as only covering public communications as it originally did. However, it should be noted at this point that the obligation to cooperate only applies – apart from access and host providers – to providers of public communications services (Section 92 Subsection 3 No. 1 TKG 2003).[82]

---

[80] ErlRV 17 BlgNR XXVI. GP, 8.

[81] ErlRV 17 BlgNR XXVI. GP, 8.

[82] See Chapter III.B.5.

Furthermore, pursuant to Section 134 No. 3 StPO, a surveillance of messages and information sent, transmitted or received by natural persons can not only be conducted on communications networks, but also on information society services (Section 1 Subsection 1 No. 2 NotifG 1999).[83] The latter is understood to be any service normally provided for remuneration by electronic means, at individual request of a recipient and at a distance, meaning that the parties are not simultaneously present. The new definition of surveillance of messages still includes a reference to Section 1 Subsection 1 No. 2 NotifG 1999. Under the old legal framework, this reference was essential as the indirectly used Section 3 Subsection 9 TKG 2003 expressly excluded any information society services from the term "communications service" that did not consist wholly or mainly in the transmission of signals on communications networks.[84] Under the current legal framework the reference remains necessary as Section 134 Subsection 3 StPO refers to the term communications network as defined by Section 3 No. 11 TKG 2003, which might be too narrow. Thus, information society services (Section 1 Subsection 1 No. 2 NotifG 1999) were generally included in the law even though there may (again) be actual overlap with the term communications network.

Following the model of the German Telecommunications Act, the wording "send, transmit and receive" is designed to ensure that all types of transmission are covered.[85]

3. Special protection of confidential communication content

Section 144 StPO protects the professional secrecy of clergymen and certain professional secrets. This section is central for privileged information in the context of the interception of content under the StPO, but also in the context of other investigation measures mentioned in this report.

Law in other areas, e.g., fiscal criminal law for fiscal criminal proceedings before courts (Section 195 Subsection 1 FinStrG), generally refers to the StPO provisions. Section 38 Subsection 2 No. 1 Banking Act[86] (*Bankwesengesetz*, BWG)[87] sets out that there is no obligation to maintain banking secrecy towards the public prosecutor and criminal courts with regard to criminal proceedings upon authorisation by a court (Section 116 StPO); and towards fiscal authorities with regard to criminal

---

[83] Annex 1 to the Notification Act 1999 includes a non-exhaustive list of services not covered by this definition.

[84] See detailed discussion by *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 44 et seq.

[85] ErlRV 17 BlgNR XXVI. GP, 8.

[86] Section 38 Subsection 5 BWG sets out that this is a constitutional provision.

[87] BGBl 532/1993 idF BGBl I 37/2018.

proceedings already instituted in relation to intentionally committed fiscal misdemeanours (with the exception of fiscal infringements).

a) Protection of professional secrecy of clergymen pursuant to Section 144 Subsections 1 and 3 StPO

The provision on the protection of professional secrecy of clergymen refers to Section 155 No. 1 (correct: Subsection 1 No. 1) according to which clergymen are exempt from being examined as witnesses on something that was revealed to them during confession or under the seal of confidentiality. If they are examined as witnesses in violation of this provision, their testimony would be null and void. These provisions are not only designed to protect confidential information, but also the individuals who confide information to the clergy; and they reflect constitutional aspects like the *nemo tenetur* principle and the protection of the rights of defence.[88]

Clergymen are understood to mean persons who perform pastoral duties in a church or religious community established in Austria and who, under internal rules, are obliged to secrecy.[89] A church or religious community is considered established if it has numerous followers in Austria irrespective of the fact whether it is officially recognised.[90]

Section 144 Subsection 1 sentence 1 StPO also protects the professional secrecy of clergymen (exemption from being examined as a witness) and declares results obtained through the circumvention of it null and void.

According to Section 144 Subsection 3 StPO a circumvention is however not prohibited if the clergymen themselves are under strong suspicion[91] of having committed an offence. Yet, as set out by Section 135 Subsection 3 StPO – and as is the case for measures of investigation pursuant to Section 135 Subsections 2 and 2a[92] and Section 135a StPO[93] – the public prosecutor has to request authorisation from the Legal Protection Commissioner[94] (Section 147 Subsection 2 StPO)[95] to

---

[88] See *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 144 mn. 2 with further references (currentness: November 2011).

[89] See detailed discussion by *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 144 mn. 4 et seqq. with further references.

[90] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 144 mn. 2 with further references (currentness: April 2015); *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 144 mn. 4 with further references.

[91] For more on "strong suspicion" see Chapter III.C.2.

[92] See Chapter III.C.2. and 3.

[93] See Chapter III.D.

[94] Section 47a StPO.

[95] See *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 147 mn. 7 (currentness: November 2011).

order and carry out interception measures[96]. If the interception of content is carried out without such authorisation, the results obtained may not be used as evidence and, if used, would be null and void because the measure was not lawfully ordered and authorised (Section 140 Subsection 1 No. 2 StPO).[97]

b) Protection of certain professional secrets pursuant to Section 144 Subsections 2 and 3 StPO

Section 144 Subsection 2 StPO stipulates that the surveillance of messages is unlawful if it is used to circumvent the right of members of certain professional groups, set out in Section 157 Subsection 1 Nos. 2 to 4 StPO, to refuse to testify. These include:

– defence counsels, attorneys-at-law, patent agents, lawyers who provide counsel in proceedings of inquiry committees of the National Council, notaries public and professional accountants with regard to information they learned in their professional capacities (Section 157 Subsection 1 No. 2 StPO);

– specialists in psychiatry, psychotherapists, psychologists, probation officers, registered mediators pursuant to the Civil Law Mediation Act, BGBl I 29/2003, and staff of recognised institutions for psychosocial counselling and care with regard to information they learned in their professional capacities (Section 157 Subsection 1 No. 3 StPO);

– media owners (publishers), media staff and employees of a media company or media services with regard to questions that relate to the individual who authored, submitted or was the informant for the programmes/articles and records; or that relate to communications they receive in view of their occupation (Section 157 Subsection 1 No. 3 StPO).

The focus of this provision is the same as the focus of Section 144 Subsection 1 StPO: they both protect professional secrets and legitimate expectations. However, in Section 144 Subsection 2 StPO, there is no indication that failing to comply with the relevant provisions has the effect that results are null and void; but, against the background of Section 157 Subsection 2 StPO, this may only be a drafting error and, thus, the results obtained through the circumvention of the prohibition are null and void.[98]

Section 144 Subsection 3 StPO applies here as well: a circumvention is lawful if the aforementioned person under a strong suspicion of having committed an

---

[96] See Chapter III.B.10.b).

[97] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 144 mn. 10.

[98] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 144 mn. 8; *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 144 mn. 16 et seq. with further references.

offence (see Chapter III.B.3.a).[99] Once a privileged person (Section 157 Subsection 1 Nos. 2 to 4 StPO) has actually been accused of an offence, they no longer have the right to refuse to testify and, thus, a circumvention of the prohibition is not an issue.[100]

In the context of measures under Section 135 Subsection 3 StPO and (the new) Section 135a StPO, the legal protection commissioner may only approve the surveillance of computer systems used exclusively for the exercise of an occupation by one of these persons if there are powerful reasons in support of the proportionality of such a measure (Section 147 Subsection 2 StPO).

According to Section 147 Subsection 1 No. 5 StPO, it is the duty of the legal protection commissioner to examine and check the order, authorisation, approval and implementation of the investigation measures under Section 135 Subsections 2, 2a and 3 StPO if these measures concern persons who have the right to refuse to testify (Section 157 Subsection 1 Nos. 2 to 4 StPO).[101] As the respective provision explicitly refers to Section 144 Subsection 3 StPO, the provision also has to be applied to investigation measures that concern clergymen.[102]

Section 147 Subsection 3 StPO sets out that the legal protection commissioner has the right to appeal against the judicial authorisation within the time-limit open to the accused for bringing an appeal (Section 87 Subsection 1 StPO).

Pursuant to Section 93 Subsection 5 TKG 2003, obligations to maintain secrecy (Section 144 StPO), the prohibition of the circumvention thereof and editorial confidentiality (Section 31 Mediengesetz) are to be observed. Providers are not required to examine the respective aspects.

4. Performance of telecommunication interception

For information on the technical enforcement of interception measures and on the respective cooperation duties of providers, please see Chapter I.A.3. and Chapter III.B.5.

Due to these (broad) cooperation duties of providers, accompanying investigative measures will only be needed in the case of surveillance of encrypted messages (see Section 135a Subsection 3 StPO; information on this provision is provided below in Chapter III.D.).

---

[99] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 144 mn. 9; *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 144 mn. 18 et seqq.

[100] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 144 mn. 9; *Kirchbacher*, in: Fuchs/Ratz (eds.), WK StPO § 157 mn. 33 with further references (currentness: October 2013).

[101] See Chapter III.B.10.b).

[102] *Reindl-Krauskopf*, in:Fuchs/Ratz (eds.), WK StPO § 147 mn. 1; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 147 mn. 2 (currentness: April 2015).

5. Telecommunication service providers' duties to cooperate

Based on a lawful information on data of a message transmission and a judicially authorised duty of cooperation, Section 138 Subsection 2 StPO sets out that providers (as defined by Section 92 Subsection 3 No. 1 TKG 2003) and other providers of services (Sections 13, 16 and 18 Subsection 2 ECG) have to provide information (Section 135 Subsection 2 StPO[103]) and assist in implementing measures required for the interception of communication (Section 135 Abs 3 StPO) without delay. Furthermore, they have to comply with orders pursuant to Section 135 Section 2b StPO[104] without delay and delete data that, until then, was not to be deleted (Section 99 Subsection 2 No. 4 TKG 2003) after the expiry of the time limit set in the order, or upon an order of the public prosecutor.

Section 94 TKG 2003 sets out the comprehensive cooperation duties of providers (i.e., operators of public communications services; as defined by Section 92 Subsection 3 No. 1 TKG 2003) in the interception of communications pursuant to the StPO: according to Section 94 Subsection 1 TKG 2003 and the ÜVO[105], they have to make available necessary facilities; Subsection 2 stipulates the specific cooperation duty. Section 94 Subsection 3 TKG 2003, the ÜVO and the Data Security Ordinance *(Datensicherheitsverordnung)*[106] specify general technical standards that are to be observed, in particular those relating to data security.

Providers are entitled to reimbursement of their expenses (Section 94 Subsections 1 and 2 TKG 2003). The Reimbursement of Investment Costs Ordinance *(Investitionskostenersatzverordnung)*[107] and the ÜKVO[108] set out details.

A provider who fails to comply with the duty to make available the necessary facilities commits an administrative offence under Section 109 Subsection 4 No. 7 TKG 2003 and is subject to a fine of up to 58,000 Euro. Such non-compliance is not punishable in cases where the investment costs have not yet been reimbursed on the basis of the respective ordinances. Where providers fail to comply with their duty to cooperate (Section 94 Subsection 2 TKG 2003), they are liable to a fine under Section 109 Subsection 3 No. 14 TKG 2003 of up to 37,000 Euro. As of 1 June 2018 providers are liable to a fine of the same amount where they transmit data unencrypted over a communications network (Section 109 Subsection 3

---

[103] See Chapter III.C.2.

[104] See Chapter III.C.4.

[105] See detailed discussion by *Pachinger*, in: Riesz/Schilchegger (eds.), TKG. Telekommunikationsgesetz Kommentar (2016) § 94 mn. 33 et seqq.

[106] BGBl II 402/2011 idF BGBl II 228/2016; see detailed discussion by *Pachinger*, in: Riesz/Schilchegger (eds.), TKG § 94 mn. 44 et seqq.

[107] BGBl II 107/2012; see detailed discussion by *Pachinger*, in: Riesz/Schilchegger (eds.), TKG § 94 mn. 20 et seqq.

[108] See detailed discussion by *Pachinger*, in: Riesz/Schilchegger (eds.), TKG § 94 mn. 27 et seqq.

No. 22 TKG 2003) and, thereby, fail to comply with Section 94 Subsection 2 TKG 2003; or where they fail to comply with Section 99 Subsection 2 No. 4 TKG 2003 and delete data specified in an order made by the public prosecutor under Section 135 Subsection 2b StPO or do not delete data when required.

Section 138 Subsection 2 StPO and Section 18 Subsection 2 ECG set out the cooperation duty of access providers (Section 13 ECG) and host providers (Section 16 ECG). Section 92 Subsection 3 and Section 111 Subsection 3 StPO apply correspondingly.

6. Formal prerequisites of interception orders

a) Public prosecutor's orders and court authorisation

The prerequisites of interception orders – and of other measures of investigation pursuant to Sections 135 and 135a StPO[109] – are set out in Section 137 Subsection 1 and Section 138 Subsection 1 StPO.

According to Section 137 Subsection 1 StPO, the public prosecutor orders investigation measures upon court authorisation (Section 86, Section 101 Subsection 2 and Section 105 StPO) – with the exception of data preservation (quick-freeze) pursuant to Section 135 Subsection 2b StPO where only the public prosecutor's order is required (Section 102 StPO)[110]. During the main trial, once the indictment has been lodged, it is the respective court that is competent to order investigation measures (Section 210 Subsection 3 StPO); in proceedings where there is a jury, the decision on orders outside the court hearing rests with the presiding judge (Section 32 Subsection 3 StPO).[111] If the surveillance of encrypted messages requires access to premises (Section 135a Subsection 3 StPO), court authorisation has to be obtained in each individual case.[112]

According to Article 10a StGG which reserves relevant decisions to judicial actors, even in exigent circumstances, the criminal police have no authority to conduct surveillance of (encrypted) messages on their own initiative.[113]

Pursuant to Section 138 Subsection 1 StPO, the order issued by the prosecutor – including those pursuant to Section 135 Subsection 2b StPO – and the authorisation by court (both required by Section 137 Subsection 1 StPO) have to specify the pro-

---

[109] Section 135a StPO will enter into force on 1 April 2020.

[110] See Chapter III.C.4.

[111] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 23 (currentness: December 2014); *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 26 (currentness: April 2015).

[112] See Chapter III.D.

[113] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 23; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 24. See also Chapter II.A.1.

ceedings, the name of the accused person, the offence the accused is suspected of, the legal denomination of the offence, and a statement justifying the application of the measure and outlining why the measure – in the individual case[114] – is proportionate (Section 5 StPO). Additionally, both order and authorisation have to provide information on the rights of the individual affected by the measure.

The indication of the actual name of the accused person is not mandatory provided there is strong suspicion against a certain person.[115]

Furthermore, the following information has to be included:

– names or other identifiers of the owner of the technical equipment that was or will be the source or destination of a message transmission; of the owner or the person authorised to dispose of the computer system on which software to facilitate the surveillance of encrypted messages will be installed; or of the person to be surveilled (No. 1),
– premises it is envisaged the investigation measure will be carried out in or the computer system on which software to facilitate the surveillance of encrypted messages will be installed (No. 2),
– message transmission type, technical equipment […] (No. 3),
– start date and end date of the interception (No. 4), and
– premises that may be accessed on the basis of the order (No. 5).

The investigation measure remains lawful, if the actual name of the owner[116] of the technical equipment cannot be specified (No. 1), e.g., the name of the anonymous[117] owner of a prepaid mobile phone.[118]

No. 3 sets out that – if known[119] – the technical equipment that is going to be surveilled (telephone number, IMEI number, IMSI number, IP address) has to be

---

[114] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 28 with further references.

[115] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 27; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 31a. Accordingly, against the background of Section 135a StPO and referring to the aspect that this is an "implementing provision" ErlRV 17 BlgNR XXVI. GP, 15 with further references.

[116] For the term owner see Chapter III.C.2.

[117] It has to be mentioned that due to Section 97 Subsection 1a TKG 2003, which entered into force 1 January 2019, there will be no anonymous owners of prepaid mobile phones any time soon: Providers are obliged to register names, academic titles and dates of birth of their subscribers upon conclusion of the contract. This also applies to contracts on prepaid mobile phones. Furthermore, providers are obliged to register the data mentioned above of those subscribers, whose data has not been registered yet (due to a contract concluded earlier than 1 January 2019). For details see Section 97 Subsection 1a TKG 2003.

[118] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 26; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 31a.

[119] ErlRV 17 BlgNR XXVI. GP, 15 explains that it is sufficient to indicate the computer system type – e.g., laptop, smartphone of the person to be surveilled.

indicated.[120] *Reindl-Krauskopf*[121] comes to the conclusion that it is appropriate to consider telephone device and SIM card to be a unit and as such technical equipment for communications under the law. Currently there is a discussion[122] whether transmitter sites may be subjected to interception. *Reindl-Krauskopf* holds the view that these stations cannot be considered to be technical equipment as they are not the source or destination of a message transmission. Thus, such measures may not be applied.[123] The legislator holds that the recent reformulation of No. 3 ("terminal equipment" is no longer listed) will avoid ambiguities.[124] It remains doubtful that it does.

If an interim step has to be taken to clearly identify the respective technical equipment (e.g., find out the IMEI number of the mobile phone used), this step can be included in the order/authorisation, however it has to be clear what technical equipment will be subjected to interception.[125]

b) "Orders addressed to operators"

Pursuant to Section 138 Subsection 3 StPO, it is the duty of the public prosecutor (where necessary upon court authorisation, which in the cases of Section 135 Subsections 2 and 3 StPO has to be indicated in the order, but not enclosed)[126] to issue a separate order that is addressed to the operator, provider or another provider of services and delivered by criminal police. The order has to provide details on the extent of the duties involved, the obligation to maintain secrecy and the information relevant for the actual implementation of the interception measure, in particular its start and end date. Start and end date may be determined by the public prosecutor (Section 101 Subsection 3 StPO) within the period for which court authorisation was given.[127] If operators, providers or other providers of services acted

---

[120] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 32; see detailed discussion by *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 30.

[121] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 30.

[122] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 32.

[123] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 32 with further references.

[124] ErlRV 17 BlgNR XXVI. GP, 15 referring to OGH 05.03.2015, 12 Os 93/14i, 12 Os 94/14m.

[125] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 33; see detailed discusscion by *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 34 et seqq.

[126] For more on the respective practical aspects see *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 40.

[127] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 41 with further references.

without such order, they would commit an offence, e.g., under Section 108 TKG 2003.[128]

Section 138 Subsection 3 last sentence StPO in connection with the reference therein to Section 93 Subsection 2 StPO allows the use of injunctions and coercive measures to ensure compliance with the order and, thus, with the duties to cooperate imposed by Section 138 Subsection 2 StPO.[129] This, however, requires written form and hand delivery of the document.[130]

Those obliged by the duty to cooperate have no right to appeal (Section 87 Subsection 1 StPO) against the court authorisation of the order, they, however, can use the remedy pursuant to Section 106 StPO claiming their rights have been violated by the order.[131]

7. Substantive prerequisites of interception orders

Section 135 Subsection 3 StPO specifies the respective requirements and sets out four circumstances/groups of cases in which the interception of content is lawful:

a) Interception of content in relation to kidnapping or hostage taking

An interception of content in relation to kidnapping or hostage taking is subject to Section 135 Subsection 2 No. 1 StPO.[132]

b) Interception of content with consent of the owner

Pursuant to Section 135 Subsection 2 No. 2 StPO, an interception of content with the consent of the owner is lawful if the owner of the technical equipment, which was or will be the source or destination of the message transmission, has consented to its surveillance.[133]

Both provisions specify how consent has to be given. The actual wordings, however, are not fully identical. Section 135 Subsection 2 No. 2 StPO requires that the owner has **expressly** consented to information on message transmissions. Although

---

[128] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 42.

[129] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 27; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 37.

[130] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 42.

[131] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 44 et seq. with further references (that partly include different opinions, but he presents powerful counter-arguments); *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 44 with further references (that partly include different opinions).

[132] See Chapter III.C.2.

[133] See Chapter III.C.2.

Section 135 Subsection 3 No. 2 StPO refers to the above provision and its scope of application, it repeats the part on the consent of the owner, but without the "expressly." Without further comment, academic literature,[134] however, assumes that he requirements in both provisions are fully identical and claims that the owner's consent to an interception of content under Section 135 Subsection 3 No. 2 StPO has to be express. Bearing in mind the extent and the intensity of the intrusion, this conclusion is correct, but the question remains: what is the reason for the difference in the wording? Perhaps it was simply a drafting error. Following this interpretation, implied, presumed or subsequent consent is not enough.

c) Interception of content without consent of the owner[135]

Pursuant to this provision, a surveillance of messages is lawful if it appears necessary for the investigation of intentionally committed offences carrying a prison sentence of more than one year, or if investigation or prevention of offences committed within a criminal or terrorist association or criminal organisation (Sections 278 to 278b StGB) would be made considerably more difficult; and, in both of these cases, if all the requirements laid down by Section 135 Subsection 3 No. 3 lit. a or lit. b StPO are fulfilled. These provisions include various groups of cases; and, as there is no consent, the respective requirements are stricter.

Central to Section 135 Subsection 3 No. 3 StPO is the investigation of an offence. An interception of content may be necessary for the investigation of an offence if the anticipated evidence which is sought probably cannot be obtained by other means of investigation.[136] As regards offences relating to participation in a criminal or terrorist association or criminal organisation (Sections 278 to 278b StGB), an interception of content can also be used to prevent these offences, and the respective requirements only demand that the investigation or prevention of these offences would be made considerably more difficult (e.g., severe delays, high costs) if interception measures were not used.[137]

There are two groups of offences that fall under this provision: the first group includes intentionally committed offences carrying a prison sentence of more than one year, no matter whether the offences are specified in the core areas of criminal law or in secondary criminal law (interception of content has particular practical

---

[134] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 27, 33 (currentness: April 2016); *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 135 mn. 30 et seq. (currentness: April 2015).

[135] This provision includes the main case of application of an interception of content (*Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 34.

[136] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 135 mn. 34; *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 36.

[137] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 42; *Ohrnhofer* in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 135 mn. 35.

relevance in the area of offences related to drugs).[138] The second group includes offences under Sections 278 to 278b StGB (Criminal association, Criminal organisation, Terrorist association). Contrary to the first group of offences, no reference is made to the penalty or mental elements of the offence; furthermore, surveillance of messages can be used to investigate and to prevent these offences.

Section 135 Subsection 3 No. 3 lit. a and lit. b StPO require strong suspicion of an offence (for both the conduct and the mental elements of the offence), i.e., the probability that a person is involved in an offence has to be greater.[139] What follows from this is that an interception in the context of Sections 278 to 278b StGB requires that there is suspicion not only of the offence relating to participation in a criminal or terrorist association or criminal organisation but also suspicion of the offence that was committed or planned as a member of this organisation/association.[140]

Section 135 Subsection 3 No. 3 lit. a StPO sets out the requirements for a lawful interception of owners of technical equipment who are under serious suspicion and whose technical equipment was or will be the source or destination of a message transmission. The addressees are identical to those in Section 135 Subsection 2 No. 2 StPO.[141]

Section 135 Subsection 3 No. 3 lit. b StPO specifies the other alternative. A surveillance is lawful if there are certain facts, i.e., grounds, that give reason to believe someone under strong suspicion of such offences will use technical equipment or establish a connection to technical equipment.

"Use" is understood to mean establishing a communication connection from technical equipment or receiving communication on it, e.g., make or answer telephone calls on it.[142]

"Establish a connection to technical equipment" is understood to mean actively establishing a communication connection to technical equipment (by the suspected person). This does not include, e.g., the answering of incoming telephone calls by

---

[138] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 24; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 135 mn. 12.

[139] See OGH 11 Os 54/97, 12 Os 12/07t = SSt 2007/7 = EvBl 2007/63 = RZ 2007/25 and others (RS 0107304); *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 135 mn. 33 with further references; *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 37 with further references, argue that the degree of suspicion has to be equal to that which justifies pre-trial detention and consider suspicion to be strong if it is very likely that an offence has been committed by the suspected person. For more on "strong suspicion" see Chapter III.C.2.

[140] See detailed discussion in *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 43 et seq.

[141] For more on the term owner see Chapter III.C.2.

[142] *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 38 et seq.; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 135 mn. 37.

suspected persons, because, in this case, they do not actively establish the connection.[143]

d) Interception of content to determine the whereabouts

An interception of content to determine the whereabouts is subject to Section 135 Subsection 2 No. 4 StPO.[144]

In addition, any surveillance of messages has to be proportionate (Section 5 StPO), giving consideration to the general degree of intrusion of this means of investigation (interception of content) but also to the degree of intrusion in the individual case (Section 135 Subsection 3 Nos. 1 to 4 StPO).[145] Consideration also has to be given to whether the intrusion on rights of third parties not involved in the offence is proportionate to the severity of the offence, the degree of suspicion and the expected results (Section 5 Subsection 1 at the end StPO).[146]

8. Validity of interception orders

According to Section 137 Subsection 3 StPO, investigation measures pursuant to Section 135 and Section 135a StPO – with the exception of a measure pursuant to Section 135 Subsection 2b StPO[147] – may only be ordered for such a future period of time (in the cases of Section 135 Subsection 2 StPO also for a past period of time) that is likely to be required in order to fulfil the respective purpose. The provision on data preservation (quick-freeze) pursuant to Section 135 Subsection 2b StPO sets out the same requirement relating to the purpose of the measure, however, this measure may be ordered for a maximum period of 12 months and a further order cannot be made. The other cases allow a further order whenever it is to be expected, on account of certain facts, that the further implementation of the investigation measure will lead to the expected success.

The wording in Section 135 Subsection 3 Nos. 2 and 3 StPO that, amongst other things, refers to technical equipment that was or will be the source or destination of

---

143 *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 39 et seq. with further references; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 135 mn. 37 with further references. Different – albeit a decision under the old legal framework – OGH 12 Os 152/00 = SSt 63/121 = JBl 2001, 531 and others, which, however, would go too far.

144 See Chapter III.C.2.

145 *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 25 et seq.; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 135 mn. 28.

146 For detailed discussion and further references to literature and case law see *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 135 mn. 26; and, in particular, for more on the surveillance of messages in the context of offences relating to participation in a criminal or terrorist association or criminal organisation mn. 44.

147 See Chapter III.C.4.

a message transmission gives rise to the question as to whether such interceptions of content are indeed restricted to the investigation of future communications in the relevant context. It has been argued in literature that the surveillance of messages for a period in the past is lawful.[148] When Section 135a was introduced to the StPO the legislator, however, explained that the surveillance of encrypted messages can only be ordered for a future period of time and that past data not related to the transmission shall not be accessed (in clear distinction to online searches).[149] Time will show whether this will end discussions on the lawfulness of the surveillance of messages for a period in the past as the wording in Section 135 Subsection 3 Nos. 2 and 3 StPO remains problematic.

If requirements for the respective investigation measure – including proportionality and purpose – cease to be satisfied, the measure must be discontinued (Section 137 Subsection 3 last sentence StPO). During investigation proceedings, the public prosecutor is competent to make such orders; where, e.g., intercepted accused persons have been arrested, the criminal police itself may discontinue the measure.[150] The prosecution has to inform the court where a measure that was judicially authorised is not implemented (Section 101 Subsection 3 StPO).

9. Recording and reporting requirements

The only recording duties set out in the StPO are those under Section 145 Subsection 4 StPO relating to the new investigation measure pursuant to Section 135a StPO: during the implementation of the surveillance measure complete and comprehensible records of the actions taken have to be kept in order to ensure the authenticity and integrity of the results obtained.[151] After termination of the measure, the software used has to be deleted and made inoperative.

According to Section 138 Subsection 4 StPO, the public prosecutor has to examine the results of the investigation measure, i.e., the data and information obtained through the respective investigation measure (a detailed definition is set out in Section 134 No. 5 StPO). In the context of the surveillance of messages, this is the messages and information sent, transmitted and received (No. 3).

It is the duty of the prosecutor to have the parts that are of significance for the proceedings and that may be used as evidence (Section 140 Subsection 1, Section 144, Section 157 Subsection 2 StPO) transformed into images or writing and file them in the case file.[152]

---

[148] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 27; *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 24 with further references.

[149] ErlRV 17 BlgNR XXVI. GP, 15.

[150] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 29.

[151] ErlRV 17 BlgNR XXVI. GP, 15 et seq.

[152] See Chapter III.E. for information about specific regulations on use/admissibility of electronic communication data as evidence in court proceedings.

Section 145 Subsection 1 StPO sets out that the public prosecutor has to retain the results of investigation measures – generally, not only in the case of investigation measures in the area of telecommunications – and submit all of them to the court when the indictment is lodged. When a final decision becomes binding, the results are to be deleted by the court unless they are used as evidence in other pending proceedings. Where the case is closed and no further action taken, it is the prosecutor's duty to do so.[153] Results transformed into images or writing and filed in the case file are not to be destroyed.[154]

Orders, judicial authorisations and results (as defined by Section 134 No. 5 StPO) that were transformed into images or writing have to be kept separately (Section 145 Subsection 2 StPO) and where required (Section 135 Subsections 2, 2a and 3 StPO, Section 135a StPO) as classified information. Details are outlined in the Classified Information Ordinance *(Verschlusssachenverordnung)*.[155] As specified in the ordinance, the entire record of the investigation is to be considered classified if there are reasons to support such a classification.

Non-compliance with Section 145 Subsection 2 StPO is an offence under Section 301 Subsection 3 StGB (Unlawful publication of proceedings).[156]

The documents listed above are to be filed in the (regular) case file when the respective order has become binding on the accused person; at the latest when the indictment is lodged.

See Chapter III.B.5. for more on the specific deletion duties under Section 99 Subsection 2 No. 4 TKG 2003 and the respective administrative offence.

See Chapter III.B.10. and 11. for more on data deletion and destruction of records.

10. Notification requirements and remedies

a) Rights of the accused person and of other persons concerned

After termination of the investigation measure, the public prosecutor has to serve the order and, where applicable, the judicial authorisation upon the accused person and upon persons affected by the measure without delay. Service may be postponed for as long as it would jeopardise the purpose of these or other proceedings

---

[153] *Ohrnhofer* in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 145 mn. 1 (currentness: April 2015); *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 145 mn. 2 et seq.

[154] For a clear view see *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 145 mn. 2 with further references; coming to the same conclusion *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 145 mn. 3.

[155] BGBl II 3/2015; see detailed discussion by *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 145 mn. 5a.

[156] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 145 mn. 8 (currentness: November 2011). There are no records concerning the practical relevance of this provision.

(Section 138 Subsection 5 StPO). The duty to serve the respective documents – and the duty to inform of the rights pursuant to Section 139 Subsection 2 and Subsection 4 StPO – applies where the identity of the persons is known or can be established without particular effort[157] (see Section 139 Subsection 2 StPO).[158] The rights of defence and the principle of proportionality set limits to the postponement of service. [159]

A "person concerned", as defined by Section 48 Subsection 1 No. 4 StPO, is a person whose rights are directly affected when force is ordered or applied against them; providers do not fall under this definition.[160]

With regard to the surveillance of encrypted messages (Section 135a StPO), instructions concerning the right of appeal have to include a reference to the right to claim reimbursement under Section 148 StPO.[161]

Furthermore, Section 139 Subsection 1 StPO sets out that the accused is to be given the opportunity to examine all results. During investigation proceedings – but not during the main trial – parts thereof that are not of significance for the proceedings may be excluded from this right in order to protect legitimate interests of third parties.[162]

Persons concerned may only examine results that relate to their data of a message transmission, to messages addressed to them or sent by them, to conversations conducted by them, or to images showing them (Section 139 Subsection 2 StPO).

Pursuant to Section 139 Subsection 3 StPO, the accused has the right to demand that further results be transformed into images or writing if these are of significance for the proceedings and if their use as evidence is lawful.

Furthermore, upon application of the accused or ex officio results have to be destroyed[163] if they will not be of significance for criminal proceedings or may not be used as evidence (Section 139 Subsection 4 StPO). Persons concerned have the same right with respect to the results outlined above in the context of Subsection 2.

---

[157] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 139 mn. 8 (currentness: April 2015); *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 139 mn. 8 (currentness: December 2014).

[158] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] §§ 137 to 138 mn. 43 with further references; see detailed discussion by *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 48.

[159] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 46.

[160] See detailed discussion by *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 138 mn. 49. See also 9.

[161] ErlRV 17 BlgNR XXVI. GP, 15.

[162] *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 139 mn. 3; *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 139 mn. 1.

[163] Internal regulations give guidance on destruction management; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 139 mn. 10 with further references.

During investigation proceedings, persons can assert these individual rights through the public prosecutor; the remedy pursuant to Section 106 StPO can be lodged against the prosecutor's decision. If the respective measures were ordered after the indictment had been lodged, it is the court that has review authority.[164]

The accused and persons concerned can use the remedy pursuant to Section 106 StPO to have the order of the prosecutor and the way it was carried out by the police reviewed; this remedy, however, cannot be used by them to have the order addressed to the operator reviewed. Pursuant to Section 87 Subsection 1 StPO, such persons can appeal against the judicial authorisation.[165]

b) Protection of rights

Section 147 Subsection 1 No. 2a StPO sets out that it is the duty of the legal protection commissioner (Section 47a StPO)[166] to examine and check the order, approval, authorisation and implementation of investigation measures under (the new) Section 135a StPO. The public prosecutor has to provide the documents to the legal protection commissioner without delay, i.e., immediately (Section 147 Subsection 3 StPO).[167] Pursuant to Section 147 Subsection 3 StPO, the legal protection commissioner has the right to appeal against the judicial authorisation within the time-limit open to the accused for bringing an appeal (Section 87 Subsection 1 StPO).[168]

In the context of measures under Section 135a StPO legal protection commissioners, furthermore, have the right to obtain a personal impression of the measure's implementation and the respective results at any time; in particular, it is their duty to examine whether the principle of proportionality is observed (Section 147 Subsection 3a StPO). The commissioners can request that an expert be appointed by the court to support them with their duties.

After termination of an investigation measure listed in Section 147 StPO, legal protection commissioners have the right to access the results before they are filed in the case file and may request that results be destroyed or data deleted (Section 147 Subsection 4 StPO). If the prosecution does not intend to accede to the request submitted by the commissioner, the matter has to be referred to the court by

---

164 *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 139 mn. 2; see detailed discussion by *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 139 mn. 2.

165 *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 139 mn. 5, 9, 11 et seqq.

166 See also 8.

167 *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 147 mn. 3; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 147 mn. 6 with further references.

168 See detailed discussion by *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 147 mn. 6; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 147 mn. 7a.

the prosecution. The legal protection commissioner (Section 87 Subsection 1 StPO) can then appeal the decision made by the court.[169]

These powers could cause difficulties in the area of mutual legal assistance (Section 50 Subsection 3 Extradition and Mutual Assistance Act (*Auslieferungs- und Rechtshilfegesetz*, ARHG),[170] where, e.g., the surveillance of a person that is currently located in Austria is carried out from abroad.[171]

11. Confidentiality and reliability requirements

See Chapter III.B.5., 6.b) and 9. for remarks on confidentiality and reliability requirements.

C. Collection and Use of Master, Access, Traffic and Location Data

1. Information on master and access data (Section 76a StPO)

Section 76a StPO provides information on master and access data. Operators of communication services must provide information on a subscriber's master data (as defined in Section 92 Subsection 3 No. 3 TKG 2003) to the criminal police, public prosecutors and courts to clarify a suspected criminal offence at their request (Section 76a Subsection 1 StPO in connection with Section 90 Subsection 7 TKG 2003). The request is not an order and does not have to be substantiated.[172]

Under Section 92 Subsection 3 No. 3 TKG 2003, the term "master data" means all data, including personal data, required for establishing, processing, modifying and/or terminating the legal relationship between the user and the provider. "Master data" also encompasses data used for the production and publication of subscriber directories. These include:

a) name (person's first name and surname; company or organisation's name in the case of legal entities),
b) a person's academic degree,
c) address (person's residential address; place of establishment or billing address in the case of legal entities),
d) subscriber number and other contact information,

---

169 *Reindl-Krauskopf* in: Fuchs/Ratz (eds.), WK StPO § 147 mn. 12 et seqq.; *Ohrnhofer*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 147 mn. 8.

170 BGBl 529/1979 idF BGBl I 32/2018.

171 *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 147 mn. 2.

172 *Kroschl*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 76a mn. 2 (currentness: March 2013).

e) information about the type of contractual relationship,

f) creditworthiness,

g) date of birth (as of 1 January 2019; BGBl I 29/2018).

The request has to be in writing (Section 90 Subsection 7 TKG 2003). In urgent cases, such requests may be carried out orally, but purely on a preliminary basis.

The situation is similar with regards to information on access data. In accordance with Section 92 Subsection 3 No. 4a TKG 2003, the term "access data" means traffic data which is created by the operator during access by a subscriber to a public communications network. This data is required for assignment to the subscriber of the network addresses used for a communication at a specific point of time.

Section 76a Subsection 2 StPO describes the access data of a person who owns technical equipment. The data as listed below can be subject to interception:

1. name, address and subscriber identification to whom a public IP address was assigned at a certain time, unless this would include a greater number of subscribers. The time zone of the person(s) is taken into consideration;
2. the subscriber identification, which is assigned to the subscriber for using e-mail services;
3. name and address of the subscriber, to whom an e-mail address was assigned at a certain time, and
4. the e-mail address and the public IP address of the sender of an e-mail.

It should be pointed out that, if a specific IP address is assigned to a subscriber for exclusive use for the duration of a contract, the IP address simultaneously constitutes master data as defined under Section 92, Subsection 3, No. 3 TKG 2003 (Section 92 Subsection 3 No. 16 last sentence TKG 2003).

Other than in the case of master data, providers of communication services have to inform on access data only upon the order[173] of the public prosecutor under Section 102 StPO (Section 76a, Subsection 2, StPO in conjunction with Section 99 Subsection 5 No. 2 TKG 2003) and only to clarify a concrete suspicion of a crime (according to Section 48 Subsection 1 No. 2 StPO). Indeed, an initial suspicion is not enough. In the main proceedings, the competent court may order this measure (Section 210 Subsection 3 StPO and Section 99 Subsection 5 No. 2 TKG 2003).

Compared to information on data of a message transmission (Section 135 Subsection 2 StPO), the measure provided in Section 76a, Subsection 2 StPO is a minor intervention. Indeed, the investigating authorities already know some traffic data, like the public IP or e-mail address. They just need to identify the owner of

---

[173] According to Section 5 Subsection 5 StAG (BGBl 164/1986 idF BGBl I 71/2014), Section 76a Subsection 2 StPO is subject to a mandatory revision.

specific technical equipment.[174] In this case, the investigating authorities will not get any information about the traffic data, which the providers have to process to discover the information. The data transfer to the investigating authorities contains only the subscriber's personal (master) data.[175]

The provisions of Section 138 Subsection 5 as well as Section 139 are to be applied correspondingly.

According to Section 138 Subsection 5 StPO, the public prosecutor shall immediately serve their order on the accused and the persons concerned via the investigative measure. However, the service may be postponed for as long as the act of serving would jeopardise the purpose of these or other proceedings.

The accused is given the opportunity to see and hear all the results (Section 139 StPO). On application by the accused, the results of the investigative measure must be destroyed. This is only carried out when the results are insignificant to criminal proceedings or not required as evidence (Section 139 Subsection 4 StPO). The persons under investigation also have the right to appeal, when the messages or images show them. This includes messages and images which are addressed to them, or sent by them, or conversations conducted by them.

As usual, if someone feels their rights have been infringed in a subjective right by the prosecutor in the investigating procedure, the person concerned may appeal against this infringement (Section 106 StPO) by such requests or orders according to Section 76a Subsections 1 and 2 StPO.

2. Information on data of a message transmission

The term "information on data of a message transmission" *(Auskunft über Daten einer Nachrichtenübermittlung)* is defined in Section 134 No. 2 StPO. It describes information on traffic data (as defined in Section 92 Subsection 3 No. 4 TKG 2003) and access data which is not covered by the request according to Section 76a Subsection 2 StPO (see above). It also encompasses location data (*Standortdaten*; Section 92 Subsection 3 No. 6 TKG 2003). Such data can be obtained from a telecommunications service, or a service of the information society (Section 1 Subsection 1 No. 2 of the Notification Act).

Essentially, this measure covers traffic data. Traffic data, according to Section 92 Subsection 3 No. 4 TKG 2003, is any data processed for the conveyance of a communications network or for billing (so-called billing data). Except in the cases regulated by the TKG 2003: the latter kind of data must not be stored or transmitted and shall be erased or made anonymous after terminating the connection (see Section 99 Subsection 1 TKG 2003).

---

174 ErlRV 1074 BlgNR XXIV. GP, 20.

175 OGH 13.4.2011, 15 Os 172/10y (15 Os 173/10w).

Traffic data may be processed for information purposes according to the following (Section 99 Subsection 5 TKG 2003):

1. data of a message transmission as per Section 134 No. 2 StPO;
2. access data to courts and public prosecutors in accordance with Section 76a Subsection 2 StPO;
3. traffic data and master data, in cases where it is necessary to process traffic data for this purpose and for the provision of information on location data to law enforcement agencies pursuant to the Security Police Act in accordance with Section 53 Subsection 3a and 3b SPG and Section 11 Subsection 1 No. 5 PStSG. In cases where it is not possible to determine a current location, the cell ID of the last communication registered by the communication equipment may be processed;
4. access data, if saved three months before the request, to law enforcement agencies pursuant to the Security Police Act in accordance with Section 53 Subsection 3a No. 3 SPG and Section 11 Subsection 1 No. 5 PStSG;
5. traffic data, access data and location data in accordance with Section 11 Subsection 1 No. 7 PStSG.

The field of criminal prosecution is relevant for information on data of a message transmission in Section 99 Subsection 5 No. 1 TKG. With this measure, the public prosecutor is able to get information on who has communicated with whom at a certain time (so-called *Rufdatenrückerfassung*) and where the person was at that time (so-called *Standortbestimmung*).

In the following cases, the principle of proportionality (Section 5 StPO) is considered. Information on data of a message transmission is admissible (Section 135 Subsection 2 StPO):

1. if and as long as it is strongly suspected[176] *(dringend verdächtig)* that one of the persons concerned has kidnapped or otherwise seized another person, and that information about data is restricted to such a message of which it has to be assumed that it was communicated, received or sent by the accused at the time when the person was deprived of his/her liberty;
2. if it is expected that this can assist in clarifying[177] an offence, committed with intent, which carries a prison term of more than six months, and if the owner

---

[176] A suspicion is strong, if it is extremely likely that the existence of a crime (committed by the suspected person) can be assumed (see *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz [eds.], WK StPO § 135 mn. 37, 48). The object of suspicion must be the crime in all its objective and subjective elements (*Fuchs*, Grundsatzdenken und Zweckrationalität in der aktuellen kriminalpolitischen Diskussion, in: Fuchs/Brandstätter [eds.], FS Platzgummer (1995) 434).

[177] This means that a certain probability for reaching relevant results is sufficient (*Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz [eds.], WK StPO § 135 mn. 23, 61).

(Inhaber) of the technical equipment;[178] which was or will be the source or the target of a message transmission, expressly agrees[179] to it,[180] or

3. if it is expected that this can assist in clarifying an offence, committed with intent, which carries a prison term of more than one year, and if it is assumed,[181] on account of certain facts, that data concerning the accused[182] can be obtained;
4. if it is to be expected, on the basis of certain facts, that information about the residence of a fugitive or absent accused person who is strongly suspected of committing a punishable act with intent, which carries a prison term of more than one year, can be obtained.[183]

The provision of information on the data of a message transmission shall be ordered by the public prosecutor on the basis of court authorisation (Section 137 Subsection 1 second sentence StPO).

Regarding Section 138 Subsection 2 StPO, providers of services are obliged to supply information on data of a message transmission immediately.

3. Localisation of a technical facility

According to Section 134 No. 2a StPO, "localisation of a technical facility" *(Lokalisierung einer technischen Einrichtung)* means the use of technical means for determining geographical locations and the IMSI number assigned to a user with-

---

Thus, other than in the case of surveillance of messages (see Chapter III.C.8.), the measure must not be necessary for clarification a punishable act.

[178] For this, the actual authority to use the equipment is crucial (*Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz [eds.], WK StPO § 135 mn. 27, 28; *Ohrnhofer*, in: Schmölzer/Mühlbacher [eds.], StPO[1.02] § 135 mn. 13). But in the view of the fundamental rights associated with this investigation measure, it shall be necessary that the person able to give his or her consent belongs to the circle of potential carriers of the secrecy of communication. The person who is admissible to give consent has to be determined in advance of the request of the prosecutor or court authorisation (see *Bergauer/Schmölzer*, Strafrecht, in: Jahnel/Mader/Staudegger [eds.], IT-Recht[3] [2012] 635 [721]).

[179] An implied or only presumed consent or a subsequent approval following the measure is not sufficient (*Ohrnhofer*, in: Schmölzer/Mühlbacher [eds.], StPO[1.02] § 135 mn. 14; *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz [eds.], WK StPO § 135 mn. 33).

[180] In this case of information on data of a message transmission, an adequate suspicion (not a strong one) is sufficient.

[181] Therefore, assumptions and speculations are not enough (see *Ohrnhofer* in: Schmölzer/Mühlbacher [eds.], StPO[1.02] § 135 mn. 18).

[182] This is always the case if the measure is likely to determine with a certain probability data of a communication link with which the accused is or was involved, e.g., the time and duration of such a communication link (e.g., e-mail address, IP address) of the accused. No "data of the accused" is such traffic data, which only relates to connections in which the accused person is not or was not involved (see *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz [eds.], WK StPO § 135 mn. 62).

[183] In this case, the strong suspicion and the suitability for determining the residence are the basic legal requirements for this measure.

out the participation of a provider (Section 92 Subsection 3 No. 1 TKG 2003) or other service provider (Sections 13, 16 and Section 18 Subsection 2 ECG). This measure has been used successfully in the form of so-called IMSI-Catchers for many years in criminal proceedings but without a specific provision. Since 1 June 2018[184], there has been a separate provision which increases legal certainty, referring to Section 5 Subsection 1 StPO.[185]

Such a localisation of a technical facility is admissible in the case of an information on data of a message transmission referring to Section 135 Subsection 2 Nos. 1, 3 and 4 only for determining geographical data and IMSI numbers, which are defined in Section 134 No. 2a StPO. In addition, this measure shall be ordered by the public prosecutor on the basis of a court authorisation (Section 137 Subsection 1 second sentence StPO).

4. Data preservation (quick-freeze)

As already mentioned above, traffic data may not be stored or transmitted except in the cases regulated by the TKG 2003. Furthermore, providers have to delete or anonymise such data immediately after termination of the connection. This provision is a major problem for criminal investigation. For that reason, the so-called data preservation *(Anlassdatenspeicherung)* or "quick freeze" is a new investigative measure brought in on 1 June 2018[186] which enables avoiding the duty of deletion of such data on the basis of an order of the prosecutor. All data which is accessible for information on data of a message transmission according to Section 135 Subsection 2 StPO can be affected by this measure (Section 134 No. 2b StPO). These are: traffic data, access data which is not covered by the request according to Section 76a Subsection 2 StPO, as well as location data of a telecommunications service or a service of the information society (see above).

Data preservation is permissible according to Section 135 Subsection 2b StPO if it seems necessary due to an initial suspicion (Section 1 Subsection 3 StPO), for safeguarding an order in compliance with Section 135 Subsection 2 Nos. 2 to 4 StPO or a request according to Section 76a Subsection 2 StPO. The data preservation shall be ordered by the public prosecutor (Section 137 Subsection 1 StPO). For the formal manner of the request, Section 102 StPO is relevant. The period in which the data in question cannot be deleted shall be quoted in this order. The measure may only be ordered for the period of time that is likely to be necessary to achieve its purpose, but for a maximum of twelve months. A new order is not permissible (Section 137 Subsection 3 StPO).

---

184 Strafprozessrechtsänderungsgesetz 2018, BGBl I 27/2018.

185 For general information about this new investigative measure see *Gölly*, jusIT 2018, 46 et seqq. and 83 et seqq.

186 BGBl I 27/2018.

The providers and other service providers immediately have to fulfil orders concerning data storage (Section 138 Subsection 2 StPO). At the end of the duration ordered by the public prosecutor, or on the basis of their specific request, the data must be deleted (Section 99 Subsection 2 No. 4 TKG 2003).[187]

After ending an investigative measure, the public prosecutor shall immediately serve their order on the accused and the persons concerned by the investigative measure. However, the service may be postponed for as long as the act of service would jeopardise the purpose of these or other proceedings. If the investigative measure was begun later or ended earlier than at the times indicated in the order, the period of the actual performance shall also be communicated (Section 138 Subsection 5 StPO).

D. Access to (Temporarily) Stored Communication Data

1. Specialised norms on source electronic communication interception by remote forensic software

On 1 April 2020, a new provision will come into force that introduces a new investigative measure for the surveillance of encrypted messages (*Überwachung verschlüsselter Nachrichten*; Sections 134 No. 3a, 135a StPO).[188] To get access to the content of encrypted messages prosecution authorities will be authorised to install remote forensic software in a computer system (as defined in Section 74 Subsection 1 No. 8 StPO, including desktop PCs and notebooks as well as other devices that make an internet connection possible like smartphones or tablets) without the knowledge of the persons concerned in specific cases of serious offences. The surveillance of encrypted messages shall be admissible:

1. if and as long as it is urgently suspected that one of the persons concerned by the information has kidnapped or otherwise seized another person, and that the information about data is restricted to such a message of which it has to be assumed that it was communicated, received or sent by the accused at the time when the person was deprived of his/her liberty, (Section 135a Subsection 1 No. 1 in connection with Section 135 Subsection 2 No. 1 StPO);
2. if it is to be expected that this can contribute to the clearing up of a punishable act, committed with intent, which carries a prison term of more than six months, and if the owner or the person authorised to dispose of the computer system, on which the forensic software shall be installed, expressly agrees to it, (Section 135a Subsection 1 No. 2 in connection with Section 135 Subsection 2 No. 2 StPO);

---

187 See also Chapter III.B.5.

188 BGBl I 27/2018.

3. if the clearing up of a crime carrying a prison term of more than ten years, or of a crime pursuant to Sections 278a – 278 e StGB,

   or the clearing up or prevention of a crime committed or planned within the framework of a criminal organisation or terrorist association, or the determination of the whereabouts of the person accused of the crimes mentioned above would otherwise be without prospects of success or be essentially impeded,

   or the clearing up of a crime against life and limb or sexual integrity and sexual self-determination carrying a prison term of more than five years would otherwise be without prospects of success or be essentially impeded,

   and

   a. the owner or the person authorised to use the computer system on which the forensic software shall be installed, is urgently suspected of such a crime mentioned above, or

   b. it is to be expected on account of certain facts, that a person who is thus urgently suspected will use or connect with the computer system, on which the forensic software shall be installed. (Section 135a Subsection 1 No. 3 in connection with Section 136 Subsection 1 No. 3 StPO).

Additionally, the surveillance of encrypted messages shall only be admissible if the forensic software is removed or deleted (e.g., by a so-called "Kill-Switch") after the investigation has ended. The computer system on which the forensic software is installed and other computer systems must not be damaged in the course of the investigative measure (Section 135a Abs 2 StPO).

In all cases, the surveillance of encrypted messages will require a court authorisation based on a reasoned order by the public prosecutor (Section 137 Subsection 1 StPO) and otherwise will be null and void according to Section 140 Subsection 1 No. 2 StPO. With regard to the admissibility in court proceedings, data obtained in this manner may only be used as evidence for the punishable act, committed with intent, for which the investigative measure was ordered or could have been ordered (Section 140 Subsection 1 No. 4 StPO, for further information see Chapter III.E.).

The installation of the remote forensic software can be done remotely or physically. If a physical installation is required, prosecution authorities will be authorised under the provision of Section 135a Subsection 3 StPO to enter a flat or another location that is protected by domestic authority and furthermore to search a container or object. With special regard to computer systems, prosecution authorities will be allowed to overcome any access protection (e.g., passwords) to install the remote forensic software. In all cases, the property and personal rights of all persons concerned shall be safeguarded to the extent possible. The legislative materials explicitly state that only the installation of software is permitted under the provision

of Section 135a StPO, which means that hardware components like certain keyloggers must not be used to get access to the content of encrypted messages.[189]

The parliamentary preparatory works also stress that the investigative measure for the surveillance of encrypted messages does not provide for means of "Online-Search."[190] According to the legal definition in Section 134 No. 3a StPO, only the surveillance of encrypted messages and information sent, transmitted or received via a communications network or an online service and the determination of linked master data, access data and traffic data will be permitted. However, there is a controversial discussion on the question whether this investigative measure borders on the means of an "Online-Search."[191]

The provision on the surveillance of encrypted messages (*Überwachung verschlüsselter Nachrichten*; Section 134 No. 3a, Section 135a StPO) will only be in force for a trial period of five years until 31 March 2025 and will then be evaluated.

2. Search and seizure of stored electronic communication data

Search and seizure of electronic communication data is a controversial issue due to the blurred borders between the provisions on surveillance of messages *(Überwachung von Nachrichten)* pursuant to Section 134 No. 3, Section 135 Subsection 3 StPO and the provisions on search and seizure pursuant to Sections 109 et seqq. and Section 117 No. 2, Sections 119 et seqq. StPO. The provisions on surveillance of messages basically apply to communication in transmission and have a higher level of protection[192] than the provisions on search and seizure, which basically apply to stored communication data.

Problems arise when electronic communication data is stored not only on the user's device but also on the communication service provider's server and when the data is only requested from the latter. The main point is that search and seizure are intended to be open investigative measures whereas the surveillance of messages can be performed in a clandestine way. Some scholars argue that the more restrictive provisions on surveillance of messages pursuant to Section 134 No. 3, Section 135 Subsection 3 StPO shall apply when stored electronic communication data is requested from the provider, referring to a need for higher protection of the user in those cases.[193] Others consider stored communication data in general as being

---

189 ErlRV 17 BlgNR XXVI. GP, 13.

190 ErlRV 17 BlgNR XXVI. GP, 2.

191 See ErlRV 17 BlgNR XXVI. GP, 8 et seqq.

192 For the requirements pursuant to Sections 134 No. 3, 135 Subsection 3 StPO in detail see Section III.B.

193 *Reindl-Krauskopf/Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 134 mn. 51 and 53; *Kroschl*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 111 mn. 13 et seq. (as at

subject to the rules of search and seizure but emphasize that the suspect needs to be informed.[194]

The distinction between access to data stored online versus access to data stored offline is also a matter of discussion. According to academic literature, only singular requests are allowed under the provisions of search and seizure. Repeated access to online-stored communication data would border on the surveillance of messages and therefore have to meet the requirements of Section 134 No. 3, Section 135 Subsection 3 StPO *(Überwachung von Nachrichten)*.[195]

The general provisions on search and seizure pursuant to Sections 109 et seqq. and Section 117 No. 2, Sections 119 et seqq. StPO are applicable to objects, including electronic data storage mediums.

A search of premises and objects (as defined in Section 117 No. 2 StPO) shall be admissible if it is to be expected, on account of certain facts, that a person suspected of a punishable act is hiding there, or that objects or traces which must be secured or processed (Section 119 Subsection 1 StPO) are in place. According to Section 120 Subsection 1 StPO, searches of a flat or another location that is protected by domestic authority, as well as the objects located therein (Section 117 No. 2 lit b StPO) shall be ordered by the public prosecutor on the basis of a court authorisation; in the case of imminent danger, the criminal police is entitled, though, to conduct these searches without any order and authorisation, for the time being. Searches of a generally inaccessible piece of land, a room, vehicle or container not protected by domestic authority may be conducted by the criminal police on their own initiative (Section 120 Subsection 2 in connection with Section 117 No. 2 lit a StPO).

"Seizure" means the preliminary establishment of control over objects and the preliminary ban on releasing objects or other property items to third parties (third-party ban) as well as the preliminary ban on selling or pledging such objects and values (Section 109 No. 1 StPO). The seizure of an object is admissible if it appears to be necessary, in the first place, for reasons of evidence (Section 110 Subsection 1 No. 1 StPO). Basically, the public prosecutor can order a seizure and the criminal police carry it out according to Section 110 Subsection 2 StPO. However, the criminal police are entitled to seize objects at their own initiative pursuant to Section 110 Subsection 3 StPO:

June 2014); see also *Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 111 mn. 17 (as at Nov. 2015).

194 *Zerbes*, ÖJZ 2012/93, 845 (851); see also *Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 111 mn. 17.

195 *Zerbes*, in: Lewisch (ed.), Wirtschaftsstrafrecht und Organverantwortlichkeit 2014, 199 (207); *Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 111 mn. 15/1.

1. if
   a. nobody has control over them,
   b. they were taken from the victim as a result of the punishable act,
   c. they were found on the site of the offence and might have been used to commit the punishable act or might have been intended to commit it, or
   d. they are of low value or can be replaced easily on a temporary basis,
2. if their possession is generally prohibited,
3. if they were found in the course of a search according to Section 120 Subsection 2 StPO, or if a person arrested for the reason of Section 170 Subsection 1 No. 1 StPO was found with them, or if they were found in the course of a search of that person pursuant to Section 120 Subsection 1, or
4. in the cases of Article 4 of the Council Regulation (EC) No. 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and measures to be taken against goods found to have infringed such rights (Official Journal No. L 196 of 02/08/2003, pages 0007 – 0014).

Section 111 Subsection 2 StPO features a special provision on the seizure of electronic data carriers:

> If information saved on data carriers is to be seized, everybody shall grant access to the information and hand over or have produced an electronic data carrier in a generally customary data format, when so requested. Moreover, he/she shall suffer the production of a back-up copy of the information saved on the data carriers.

The wording of the law is imprecise because it is not the information that is to be seized initially but rather the data carrier, such as, e.g., a smartphone, a laptop computer, a hard disc or a USB device. The information is then obtained in the course of the examination of the data carrier.

A very important question in this context is how to deal with access restrictions. Section 111 Subsection 2 StPO provides for the duty of everybody to "grant access" to the information requested. This includes the duty to hand over the necessary passwords. The duty to "grant access" however does not entail the duty to take action.[196] The duty to cooperate is not applicable to the suspect in the investigation, according to prevailing opinion considering the general right of the suspect not to give any testimony in accordance with the prohibition on self-incrimination. Furthermore, witnesses bound to professional secrecies are also considered not to be subject to the duty of Section 111 Subsection 2 StPO.[197]

---

[196] *Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 111 mn. 13.

[197] *Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 111 mn. 2, 13; *Kroschl*, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 111 mn. 11.

Prosecution authorities may even use their own decryption software when the persons concerned are informed about the proceeding.[198]

In any event, the person affected by the seizure must be issued or sent a confirmation of the seizure immediately or within 24 hours at the latest. The confirmation must also include instructions on the legal remedies available in this regard. A person is considered as "concerned," if their rights are directly affected when force is ordered or applied against them (Section 48 Subsection 1 No. 3 StPO).

E. Use of Electronic Communication Data in Court Proceedings

Intercepted electronic communication data as a "result" (Section 134 No. 5 StPO) of an investigative measure pursuant to Section 135 StPO may only be used as evidence, and will otherwise be null and void, first, if the investigative measure was lawfully ordered and authorised in accordance with Section 137 StPO, which requires a court authorisation based on a reasoned order by the public prosecutor, and second, in the cases of Section 135 Subsection 2 (concerning the information on data of a message transmission) Nos. 2 to 4 and Subsection 3 (concerning the surveillance of messages) Nos. 2 to 4 StPO only when used as evidence for the punishable act, committed with intent, for which the investigative measure was ordered or could have been ordered (Section 140 Subsection 1 Nos. 2 and 4 StPO).

The latter case concerns evidence which is related to an offence not mentioned or anticipated in the interception order and found by chance in the course of the investigation. If a review of the results leads to indications that another punishable act was committed than the one that gave rise to the surveillance, a separate file must be opened with that part of the results, if their use as evidence is admissible (Section 140 Subsection 2 StPO). The admissibility of this evidence depends on the special provision of Section 140 Subsection 1 mentioned above as well as general rules for the admissibility of evidence that protect certain rights to refuse to give evidence and remain silent (Section 144 and Section 157 Subsection 2 StPO). Data thus obtained can be used for the prosecution of individuals who were not the subject of the underlying interception order.

Pursuant to Section 138 Subsection 4 StPO, the public prosecutor shall review the material intercepted as a "result" of an investigative measure according to Section 134 No. 5 StPO and have those parts transformed into images or written form, as well as having them annexed to the files that are of significance for the proceedings and may be used as evidence.

---

[198] *Tipold/Zerbes*, in: Fuchs/Ratz (eds.), WK StPO § 111 mn. 13/1 et seqq.; *Zerbes*, in Lewisch (ed.), Wirtschaftsstrafrecht und Organverantwortlichkeit 2014, 199 (206).

After ending an investigative measure pursuant to Section 135 Subsections 2 and 3, the public prosecutor shall immediately serve his order and the court authorisation on the accused and the persons concerned by the investigative measure. However, the service may be postponed for as long as the act of service would jeopardize the purpose of these or other proceedings (Section 138 Subsection 5 StPO).

According to Section 139 Subsection 1 StPO, the accused shall be given an opportunity to see and hear all results of the investigative measures.

Upon application by the accused or ex officio, the results of the investigative measure shall be destroyed if they cannot be of significance for criminal proceedings or may not be used as evidence (Section 139 Subsection 4 StPO). The public prosecutor is responsible for deciding upon the application in the first instance. The accused may appeal to the court against the decision of the public prosecutor in accordance with Section 106 StPO.

The matter of admissibility of intercepted data obtained from foreign jurisdictions has not yet been explicitly addressed by existing law. However, there is a case in which the OGH *(Oberster Gerichtshof)* declared results of a surveillance operation obtained from foreign investigations to be admissible in the national court proceeding although the surveillance operation was conducted arbitrarily in Austria by foreign authorities not according to the provisions of national law. The OGH held that the provisions of the StPO only apply to investigations of national authorities and not to (unauthorised) investigations of foreign authorities.[199] However, the OGH left open the question whether the use of evidence obtained in this manner could have been considered null and void under the provision of Section 281 Subsection 1 No. 4 StPO which addresses violations of the guarantees under Article 6 of the European Convention of Human Rights concerning the right to a fair trial. This decision of the OGH is also viewed critically in the academic literature which argues in favour of a prohibition of the use of evidence in this case, considering the danger of circumvention of the safeguards of the StPO.[200]

These concerns also relate to evidence obtained from outside the criminal justice system, where the protection level pertaining to investigative measures is not as high as in the StPO.[201]

---

[199] OGH 25.5.2004, 14 Os 47/04.

[200] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 140 mn. 30 et seq (currentness: December 2014).

[201] *Reindl-Krauskopf*, in: Fuchs/Ratz (eds.), WK StPO § 140 mn. 32, referring to results obtained from investigative measures under the SPG.

IV. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

1. Directive 2014/41/EU regarding the European Investigation Order in criminal matters

The Directive 2014/41/EU regarding the European Investigation Order in criminal matters has been implemented at the national level in the Federal law on judicial cooperation in criminal matters with the Member States of the European Union (*Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union*; EU-JZG).[202] The provisions concerned apply from the 1 July 2018.[203]

It should be noted at this point that the Directive 2014/41/EU regarding European Investigation Order replaces, according to Article 34 No. 1, the corresponding provisions of the following conventions applicable between the Member States bound by this Directive, without prejudice to their application between Member States and third States and their temporary application by virtue of Article 35:

(a) European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 20 April 1959, as well as its two additional protocols, and the bilateral agreements concluded pursuant to Article 26 thereof;

(b) Convention implementing the Schengen Agreement;

(c) Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and its protocol.

2. International (multilateral) conventions

Austria has ratified the following international conventions:

– *European Convention on Mutual Assistance in Criminal Matters*

The European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, ratified by Austria on 31 July 1968, entered into force for Austria on 31 December 1968. The following reservations and declarations should be noted with regard to the interception of telecommunication:

Reservation to Article 1 (1):
Austria will only grant assistance in proceedings in respect of offences also punishable under Austrian law and the punishment of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities.

---

202 BGBl I 36/2004 idF BGBl I 28/2018.

203 See Section 140 Subsection 16, Section 141 Subsection 3 EU-JZG.

Reservation to Article 2 (b):
In 'other essential interests of its country' Austria will include maintaining the secrecy stipulated by Austrian legislation.

Declaration concerning Article 5 (1):
Austria will make the execution of letters rogatory for search or seizure of property subject to the condition laid down in sub-paragraph (c).

Declaration concerning Article 16 (2):
Subject to the provisions of paragraph 3 of Article 16, requests and annexed documents, which are not drawn up in German, French or English language, must be accompanied by a translation into one of these languages. A translation of information mentioned in paragraph 1 of Article 21 is not required.

Declaration concerning Article 24:
For the purpose of the Convention, Austria will regard as judicial authorities the Criminal Courts, the Department of Public Prosecution and the Federal Ministry of Justice.[204]

– *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*

Austria also ratified the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 17 March 1978, which entered into force for Austria on 31 July 1983, making the following declaration:

"According to Art. 8 para. 2 of the Protocol the Republic of Austria declares to accept Chapter I only in respect of offences in connection with taxes, duties and customs.

On the grounds of the Austrian reservation to Art. 2 para. (b) of the Convention and with a view to Art. 8 para. 1 of the Protocol, the Republic of Austria declares that mutual assistance according to Chapter I of the Protocol will be granted only under the condition that – in conformity with Austrian legislation on secrecy – information and evidence received by way of mutual assistance will only be used in the criminal proceedings for which mutual assistance was requested and in directly related proceedings in respect of offences in connection with taxes, duties and customs."[205]

– *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*

Furthermore, Austria has recently ratified the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 8 November 2001 on 10 November 2017, which entered into force for Austria on 1 March 2018.[206] Austria has made the following declarations:

---

[204] BGBl 41/1969.

[205] BGBl 296/1983.

[206] BGBl III 22/2018.

"In accordance with Article 6, Austria declares that it will regard as judicial authorities the Criminal Courts, the Public Prosecution Services as well as the Federal Ministry of Justice.

In accordance with Article 17, Austria designates the officials of the Federal Ministry of the Interior, Directorate-General for Public Security – Branch for Special Units – Central Surveillance as competent officials for the implementation of a cross-border observation.

In accordance with Section 55, paragraph 1, of the Federal Act of 4 December 1979 on Extradition and Mutual Legal Assistance, Federal Law Gazette No. 529/1979, the Austrian authority competent for granting cross-border observations is the Public Prosecution Service where crossing of the border is expected to take place or where the observation will begin; in case of an observation of an incoming aircraft, the Public Prosecution Service where landing will take place. Should determination of a competent authority not be possible under these rules, the Vienna Public Prosecution Service is the competent authority for granting cross-border observations.

In accordance with Article 18, Austria designates the officials of the Federal Ministry of the Interior, Directorate-General for Public Security – Branch for Special Units – Central Surveillance as well as the officials of the customs law enforcement authorities as competent officials for the implementation of a controlled delivery. Austria declares that the authority competent for granting requests under Article 18 is the Public Prosecution Service where crossing of the border is expected to take place or where the controlled delivery will begin.

In accordance with Article 19, Austria declares that the Public Prosecution Service where the operation is expected to begin is the competent authority for requests under Article 19.

In accordance with Article 27, Austria declares that the competent administrative authorities within the meaning of Article1, paragraph 3, of the Second Additional Protocol are the district administrative authorities having territorial jurisdiction (district chief officers' departments or bodies of a city with a status of its own); however, in matters falling within the remit of the Land police departments in a local authority area in respect of which the Land police department is also the security authority of first instance, the Land police departments as well as the local fiscal law enforcement authorities (tax and customs authorities) are the competent administrative authorities."[207]

– *EU Convention of 29 May 2000 on Mutual Assistance in Criminal Matters*

At the level of the European Union, Austria ratified the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union as well as the additional Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, which both entered into force for Austria on 3 July 2005.[208]

However, the Directive 2014/41/EU regarding the European Investigation Order in criminal matters replaces, as of 22 May 2017, the corresponding provisions of

---

[207] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/182/declarations (currentness: 23 July 2019).

[208] BGBl III 65/2005; BGBl III 66/2005.

the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and its protocol applicable between the Member States bound by this Directive (Article 34 No. 1 lit c of the Directive). Therefore mutual legal assistance with EU countries will be regulated by the Austrian law implementing the Directive 2014/41/EU regarding the European Investigation Order in criminal matters (*in concreto* by the pertaining provisions of the EU-JZG; see Section D.II.).

– *Instruments for specific areas of crime*

Regarding conventions regulating cooperation for a specific area of crime, Austria is party to the following treaties:

– Austria ratified the *United Nations Convention against Transnational Organized Crime of 15 November 2000*. It entered into force for Austria on 23 October 2004.[209]
– Austria also ratified the *Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime*, which entered into force for Austria on 8 November 2013,[210] as well as the
– *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime*, which entered into force for Austria on 15 October 2005,[211] and the
– *Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime*, which entered into force for Austria on 30 December 2007.[212]

At the European level, Austria ratified the

– *Convention on Cybercrime* of the Council of Europe of 23 November 2001, which entered into force for Austria on 1 October 2012.[213]

Austria made the following reservations and declarations that should be noted with regard to the interception of communication:

> "Austria will, in accordance with Article 29, paragraph 4, of the Convention, refuse a request for mutual assistance to order the preservation of stored computer data, as provided for under Article 16 of the Convention, if the condition of dual criminality is not

---

209 BGBl III 84/2005.
210 BGBl III 296/2013.
211 BGBl III 220/2005.
212 BGBl III 11/2008.
213 BGBl III 140/2012.

fulfilled; this does not apply to the offences established in accordance with Articles 2 through 11 of this Convention.

Austria declares that the following authority has been designated as responsible pursuant to Articles 24, paragraph 7, and 27, paragraph 2, of the Convention on Cybercrime:

Bundesministerium für Justiz (Federal Ministry of Justice)
Abt. IV 4 *Internationale Strafsachen* (International Criminal Matters)
1070 Wien, Museumstraße 7
Tel.: +43 1 52 1 52-0
Email: team.s@bmj.gv.at

Austria declares that the following authority has been designated as point of contact pursuant to Article 35 of the Convention:

Bundesministerium für Inneres (Federal Ministry of the Interior)
Bundeskriminalamt (Federal Criminal Police Office)
Büro 5.2 Cyber-Crime-Competence-Center
Josef Holaubek Platz 1
1090 Wien"[214]

Austria has signed, but not yet ratified the

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[215]

3. Bilateral treaties

In the recent past, Austria has concluded bilateral treaties on mutual legal assistance in criminal matters with the USA (BGBl III 7/2010), Croatia (BGBl III 67/2009) and Poland (BGBl III 39/2005). However, these treaties do not contain specific provisions on the interception of electronic communication.

4. National regulation on mutual legal assistance in criminal matters

Beyond the ratified treaties, national legislation basically enables non-treaty based mutual assistance in criminal matters for the interception of electronic communication in the form of general rules. The national legal basis for mutual assistance includes the following laws:

– The Federal Law of 4 December 1979 on Extradition and Mutual Assistance in Criminal Matters (ARHG) and the associated ordinance *(Verordnung des Bundesministers für Justiz vom 30. April 1980 über den Auslieferungsverkehr und*

---

[214] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations (currentness: 23 July 2019).

[215] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures (currentness: 23 July 2019).

den zwischenstaatlichen Rechtshilfeverkehr in Strafsachen [Auslieferungs- und Rechtshilfeverordnung; ARHV]);[216]

– the Federal Law on Judicial Cooperation in Criminal Matters with the Member States of the European Union (EU-JZG).

a) ARHG

The provisions of the ARHG shall be applicable only insofar as intergovernmental agreements do not stipulate otherwise (Section 1 ARHG). In accordance with the provisions of this federal law, judicial assistance may be granted in criminal matters upon a request by a foreign authority (Section 50 Subsection 1 ARHG). Neither the ARHG nor the ARHV contain specific provisions on the interception of electronic communication or the execution of a respective request. However, Sections 56 Subsection 2 and Section 58 ARHG refer to investigative measures governed by Chapter Five of Title 8 of the StPO, which also includes the interception of electronic communication.

b) EU-JZG

The EU-JZG governs the cooperation between the judicial authorities of the Republic of Austria and those of the other Member States of the European Union in criminal proceedings against natural persons and associations. This cooperation comprises the recognition and execution of European Investigation Orders (Section 1 Subsection 1 lit h EU-JZG, for details see Chapter IV.B.).

B. Procedures and Execution of Requests

1. Incoming requests

a) ARHG

Pursuant to Section 55 Subsection 1 ARHG, the public prosecutor's office with competence for the court district in which the act of judicial assistance is to be performed shall be responsible for processing a request for judicial assistance. If the request calls for a cross-border observation, the public prosecutor's officer shall be responsible in the court district in which the border is most likely to be crossed. In the case of an observation in an aircraft flying to Austria, however the public prosecutor's office shall be responsible in the court district in which the aircraft is to land. If the competences cannot be determined on the basis of the present provisions, the public prosecutor's office in Vienna shall be responsible. The stipulations

---

[216] BGBl 219/1980.

of Title 7 of the StPO shall apply similarly to the processing of requests for judicial assistance.

Section 58 ARHG rules that if judicial assistance is provided in the form of one of the investigative measures governed by Chapter Five of Title 8 of the StPO which also concerns the interception of electronic communication, the assistance shall be limited in time, on which the requesting foreign authority shall be informed through the established channels of communication. Furthermore, according to Section 56 Subsection 2 ARHG, a request for ordering and performing one of the investigative measures governed by Chapter One to Chapter Eight of Title 8 of the StPO (also including interception of electronic communication) shall comprise a copy, a certified copy or a photostat copy of the order of the competent authority. If this is not a court order, the authority requesting judicial assistance shall present a statement explaining that the prerequisites required for such measures are met under the law applicable in the requesting State. There shall be compliance with a request for judicial assistance which requires a procedure that differs from Austrian laws on criminal procedure, if this is compatible with the criminal procedure and its principles pursuant to the provisions of Title 1 of the StPO (Section 58 ARHG). Basically, the provisions of the StPO shall be applied in analogy (Section 9 ARHG). In this context the question arises whether there shall be compliance with a request for judicial assistance which requires an interception of electronic communication without court authorisation.[217]

b) EU-JZG

The general rule on competences to process a request for judicial assistance in the EU-JZG (now Section 57 Subsection 4 EU-JZG) refers to the provision of Section 55c EU-JZG, so the public prosecutor's office with competence for the court district in which the requested investigative measure is to be performed shall be responsible for processing a request for judicial assistance.

Section 55c EU-JZG, however, constitutes one of the specific provisions regarding the European Investigation Order (EIO) (Sections 55 et seqq.) which have recently been implemented in the EU-JZG and entered into force on 1 July 2018.[218]

According to Section 55c Subsection 1 EU-JZG, the public prosecutor's office with competence for the court district in which the requested investigative measure is to be performed shall be responsible for executing an EIO.

In cases of notifications according to Article 31 of the Directive 2014/41/EU ("Notification of the Member State where the subject of the interception is locat-

---

[217] Cf. *Zerbes*, in: Ambos/König/Rackow (eds.), Rechtshilferecht in Strafsachen (2015) Chapter 1 mn. 211 et seq.

[218] BGBl I 28/2018.

ed from which no technical assistance is needed"), the public prosecutor's office with competence for the court district in which the subject of the interception has been, is or will be during the interception shall be responsible for the notification. If the competent authority cannot be determined on the basis of this provision, the public prosecutor's office in Vienna shall be responsible (Section 55c Subsection 2 EU-JZG).

According to Section 55d Subsection 7 EU-JZG, the public prosecutor's office may, in cases where the interception would not be authorised under the provisions of Section 55a Subsection 1 Nos. 1 to 5, 8 and 13, notify the competent authority of the intercepting Member State, within 96 hours of the receipt of the notification, that the interception may not be carried out or shall be terminated, and that any material already intercepted may not be used.

It should be mentioned that, according to Article 30 No. 5 Sentence 1 of the Directive 2014/41/EU, Austrian legislation makes use of the option that in addition to the grounds for non-recognition or non-execution referred to in Article 11 of the Directive, the execution of an EIO may also be refused where the investigative measure would not have been authorised in a similar domestic case (Section 55a Subsection 1 No. 13 EU-JZG).[219]

Regarding the procedure and execution of such a request, the national legal provisions of the StPO apply in analogy (Section 1 Subsection 2 EU-JZG in connection with Section 9 Subsection 1 ARHG). In particular, this means that a court authorisation is required for the execution of a requested interception of electronic communication (Section 137 Subsection 1 StPO, Section 55e Subsection 2 EU-JZG).[220]

In accordance with Article 14 No. 1 of the Directive 2014/41/EU, the legal remedies of the StPO are applicable to the investigative measures indicated in the EIO (Section 55e Subsection 4 EU-JZG). As regards activities of the public prosecutor's office, an objection can be filed against a violation of a personal right according to Section 106 StPO *(Einspruch wegen Rechtsverletzung)*. Decisions of the court may be subject to a complaint according to Section 87 StPO *(Beschwerden)*.[221] However, the substantive reasons for issuing the EIO may be challenged only in an action brought in the issuing State (Article 14 No. 2 of the Directive 2014/41/EU, implemented in Section 55e Subsection 4 EU-JZG). It should be noted at this point that the parliamentary preparatory works assume, without prejudice to any future interpretation by the European Court of Justice, that this provision

---

219 See also ErlRV 66 BlgNR XXVI. GP, 7.

220 See also ErlRV 66 BlgNR XXVI. GP, 10.

221 See also ErlRV 66 BlgNR XXVI. GP, 11.

refers to reasons such as necessity, proportionality, urgency of the suspicion and similar reasons.[222]

There is no explicit duty for Austria to filter out or to delete privileged information (cf. Section III.B.3.), before transmitting the results of an interception measure to a foreign country in the respective laws on mutual assistance in criminal matters. However, it has to be taken into account that the requirements of the respective provisions of the StPO must be met with regard to the execution of the investigative measure (cf. Section 55a Subsection 1 No. 8 EU-JZG, see also Chapter III.B.3.).

According to Section 55l Subsection 3 EU-JZG, the results of surveillance of messages shall be transferred to the issuing authority on the condition that the evidence must not be used in proceedings other than those which are subject to the EIO unless the executing authority agrees on the use of this evidence in another proceeding.[223]

There are no explicit rules on the storage of communications data in connection with mutual assistance in criminal matters.

2. Outgoing requests

a) ARHG

According to Section 71 ARHG, requests for judicial assistance shall be directed, by way of the established channels of communication, to the foreign court, the foreign public prosecutor's office, or the authority engaged in the execution of punishments or measures in whose district the act of judicial assistance is to be performed. The request shall comprise the facts underlying the proceedings and other information as required for appropriate processing. The competent public prosecutor can only issue a request if the requirements of the StPO for the surveillance of messages are fulfilled. With regard to the prerequisites of the StPO, a request for the interception of electronic communication may be ordered by the public prosecutor's office based on a court authorisation.[224] Furthermore, the requirements stipulated in potentially applicable international agreements must be taken into account (cf. Section 1 ARHG: "Primacy of Intergovernmental Agreements"). Unless direct judicial assistance exchanges are in place, the Federal Minister of Justice may refrain from forwarding a request for judicial assistance for one of the reasons listed in Sections 2 and 3 ARHG (ordre public, essential interests of the Republic of Austria, reciprocity).

---

[222] See also ErlRV 66 BlgNR XXVI. GP, 11.

[223] See ErlRV 66 BlgNR XXVI. GP, 14 making reference to the option of Article 30 No. 5 Sentence 2 of the Directive 2014/41/EU.

[224] See *Martetschläger*, in: Höpfel/Ratz (eds.), Wiener Kommentar zum Strafgesetzbuch[2] ARHG § 71 mn. 1 (currentness: 1 Aug. 2016).

b) EU-JZG

An EIO may be transmitted by the public prosecutor's office (Section 56 Subsection 1 EU-JZG). The EIO itself does not require court authorisation pursuant to Section 56 Subsection 2 EU-JZG. However, the prerequisites of the national procedure law (StPO) for the interception of electronic communication remain unchanged.[225]

C. Real-Time Transfer of Communications Data

Neither the national regime on telecommunications interception nor the national law on mutual legal assistance contains special provisions on the real-time transfer of communications data.

However, by consenting to the *Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union,* Austria entered into an obligation to provide for an "immediate transmission" of telecommunications data to the requesting Member State according to Article 18 of the Convention.

Furthermore, the following provisions of the *Convention on Cybercrime* of the Council of Europe of 23 November 2001, which entered into force for Austria on 1 October 2012, should be noted at this point:

Article 33 Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

D. Statistics

No official statistics are available on the extent of requests for electronic telecommunication interception in the context of mutual legal assistance.

---

[225] ErlRV 66 BlgNR XXVI. GP, 16; for the national provisions in detail see Chapter III.

Bibliography

Bergauer, Das materielle Computerstrafrecht (2016).

Bergauer/Schmölzer, Strafrecht. In: Jahnel/Mader/Staudegger (eds.), IT-Recht[3] (2012) 635.

Berka, Verfassungsrecht[6] (2016).

Birklbauer/Hilf/Tipold, Strafrecht Besonderer Teil I[4] (2017).

Fuchs, Grundsatzdenken und Zweckrationalität in der aktuellen kriminalpolitischen Diskussion. In Fuchs/Brandstätter (eds.), FS Platzgummer (1995) 434.

Gölly, Gesetzgebungsmonitor zum sog „Sicherheitspaket": Regierungsvorlage für ein Strafprozessrechtsänderungsgesetz 2018 und Regierungsvorlage für Änderungen im Sicherheitspolizeigesetz in der Straßenverkehrsordnung 1960 und im Telekommunikationsgesetz 2003 – Teil 1, jusIT 2018, 46.

– Gesetzgebungsmonitor zum sog „Sicherheitspaket": Regierungsvorlage für ein Strafprozessrechtsänderungsgesetz 2018 und Regierungsvorlage für Änderungen im Sicherheitspolizeigesetz in der Straßenverkehrsordnung 1960 und im Telekommunikationsgesetz 2003 – Teil 2, jusIT 2018, 83.

Grabenwarter/Holoubek, Verfassungsrecht – Allgemeines Verwaltungsrecht[2] (2014).

Hinterhofer/Oshidari, System des österreichischen Strafverfahrens (2017).

Kirchbacher, in: Fuchs/Ratz (eds.), WK StPO § 157 (currentness: October 2013).

Kroschl, in: Schmölzer/Mühlbacher (eds.), StPO Strafprozessordnung Praktikerkommentar[1.02] § 5 (currentness: March 2013).

– StPO[1.02] § 76a (currentness: March 2013).

– StPO[1.02] § 111 (currentness: June 2014).

Lewisch, Criminal Law and Criminal Procedure. In: Grabenwarter/Schauer (eds.), Introduction to the Law of Austria (2015) 261.

– Verfassung und Strafrecht (1993).

Martetschläger, in: Höpfel/Ratz (eds.), Wiener Kommentar zum Strafgesetzbuch[2] ARHG § 71 (currentness: August 2016).

Öhlinger/Eberhard, Verfassungsrecht[10] (2014).

Ohrnhofer, in: Schmölzer/Mühlbacher (eds.), StPO[1.02] § 135 (currentness: April 2015).

– StPO[1.02] §§ 137 to 138 (currentness: April 2015).

– StPO[1.02] § 139 (currentness: April 2015).

– StPO[1.02] § 144 (currentness: April 2015).

– StPO[1.02] § 145 (currentness: April 2015).

– StPO[1.02] § 147 (currentness: April 2015).

Pachinger, in: Riesz/Schilchegger (eds.), TKG. Telekommunikationsgesetz Kommentar (2016) § 94.

Reindl-Krauskopf/Tipold/Zerbes, in: Fuchs/Ratz (eds.), Wiener Kommentar zur Strafprozessordnung (WK StPO), § 134 (currentness: April 2016).

– WK StPO § 135 (currentness: April 2016).

Reindl-Krauskopf, in: Fuchs/Ratz (eds.), WK StPO § 138 (currentness: December 2014).

– WK StPO § 139 (currentness: December 2014).

– WK StPO § 140 (currentness: December 2014).

– WK StPO § 144 (currentness: November 2011).

– WK StPO § 145 (currentness: November 2011).

– K StPO § 147 (currentness: November 2011).

Schloenhardt/Höpfel (eds.), Strafgesetzbuch. Austrian Criminal Code (2016).

Tipold/Zerbes, in: Fuchs/Ratz (eds.), WK StPO § 111 (currentness: November 2015).

Wiederin, in: Fuchs/Ratz (Eds.), WK StPO § 5 (currentness: October 2013).

Zerbes, Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen. ÖJZ 2012/93, 845.

– Einsatz von Spionagesoftware bei Sicherstellung und Durchsuchung. In: Lewisch (ed.), Wirtschaftsstrafrecht und Organverantwortlichkeit 2014, 199.

– in: Ambos/König/Rackow (eds.), Rechtshilferecht in Strafsachen (2015) Chapter 1 Part 4 Section 5.

List of Abbreviations

AbwA	Abwehramt (Counter Intelligence Office)
ARHG	Auslieferungs- und Rechtshilfegesetz (Extradition and Mutual Assistance Act)
ARHV	Auslieferungs- und Rechtshilfeverordnung
BGBl	Bundesgesetzblatt (Federal Law Gazette)
BKA	Bundeskriminalamt (Federal Criminal Police Office)
BKAG	Bundeskriminalamt-Gesetz (Federal Criminal Police Office Act)
BlgNR	Beilagen zu den stenographischen Protokollen des Nationalrates
BM.I	Bundesministerium für Inneres (Ministry of the Interior)
B-VG	Bundes-Verfassungsgesetz (Federal Constitutional Law)
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Federal Office for the Protection of the Constitution and the Fight against Terrorism)
BWG	Bankwesengesetz (Banking Act)

DSG	Datenschutzgesetz (Data Protection Act)
ECG	E-Commerce-Gesetz (E-Commerce Act)
EMRK	Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten/Europäische Menschenrechtskonvention (European Convention on Human Rights)
ErlRV	Erläuterungen zur Regierungsvorlage (parliamentary preparatory works)
EU-JZG	Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union (Federal law on judicial cooperation in criminal matters with the Member States of the European Union)
FinStrG	Finanzstrafgesetz (Law on Financial Crime)
GRC	Charta der Grundrechte der Europäischen Union (Charter of Fundamental Rights of the European Union)
IMSI	International Mobile Subscriber Identity
MBG	Militärbefugnisgesetz (Military Warrant Act)
mn.	margin number (Randzeichen)
HNaA	Heeresnachrichtenamt (Army Intelligence Office)
NotifG 1999	Notifikationsgesetz 1999 (Notification Act 1999)
OGH	Oberster Gerichtshof (Supreme Court)
PStSG	Polizeiliches Staatsschutzgesetz (Police State Protection Act)
RGBl	Reichsgesetzblatt (Imperial Law Gazette)
SPG	Sicherheitspolizeigesetz (Security Police Act)
StAG	Staatsanwaltschaftsgesetz (Public Prosecutor's Office Act)
StGB	Strafgesetzbuch (Austrian Criminal Code)
StGG	Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder (Basic Law on the General Rights of Nationals in the Kingdoms and Länder represented in the Council of the Realm)
StPO	Strafprozessordnung (Austrian Code of Criminal Procedure)
TKG 2003	Telekommunikationsgesetz 2003 (Telecommunications Act 2003)
ÜKVO	Überwachungskostenverordnung (Ordinance of the Federal Minister for Justice on the Refund of the Providers' Expenses for the Participation in the Information on Data of a Message Transmission, Information on Data Preservation, and the Surveillance of Messages)

ÜVO	Überwachungsverordnung (Ordinance of the Federal Minister for Traffic, Innovation and Technology on the Interception of Telecommunication)
WK StPO	Wiener Kommentar zur Strafprozessordnung (Vienna Commentary on the Code of Criminal Procedure)
ZollR-DG	Zollrechts-Durchführungsgesetz (Act to implement Customs Law)

Belgium*

National Rapporteurs:
Gertjan Boulet
Paul De Hert

* This report reflects legislation and case law as of September 2018. The authors would like to thank Ms Michaëla Roegiers for her insightful review and interviews with Federal Magistrates Frédéric Van Leeuw and Jan Kerkhofs. The authors and Michaëla Roegiers would like to express their sincere gratitude to the Federal Magistrates for their time and valuable legal feedback provided during the interviews.

Contents

I. Security Architecture and the Interception of Telecommunications

A. Law Enforcement Institutions and Security Services with Powers of Telecommunications Interception

1. National security architecture

The Belgian national security architecture includes (preventive) police law, (preventive and reactive) criminal law, and intelligence (state security) law. All of these legal regimes provide coercive powers for the interception of electronic communications.

The prerequisites under general police law for the interception of electronic communications differ from the other legal regimes, which contain stricter rules on authorization: in criminal law, prior authorization by the public prosecutor (during the preliminary investigation/inquiry phase, or during the investigation phase) or by the investigating judge (during the investigation phase) is required; in intelligence law, prior authorization (for exceptional intelligence collection methods) or *a posteriori* authorization (for specific intelligence collection methods) by the administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services (SIM commission) is required.

The prerequisites for the interception of the content of communications in transmission under criminal law and intelligence law are largely similar.[1] However, the interception powers under intelligence law provide special protection for journalists, unlike the interception powers under criminal law.

---

[1] Article 90*ter* CCP, and Article 18/17 of the Act of 30 November 1998 on the Intelligence and Security Services.

2. Powers for the interception of telecommunications[2]

a) Law of criminal procedure

aa) Normal investigation methods

The legal provisions for intercepting electronic communications under (reactive) criminal law are provided in the Code of Criminal Procedure (CCP): data seizure and non-secret (network) search (Article 39*bis* CCP), data preservation request for natural persons or legal persons (Article 39*ter* CCP), data preservation request for foreign authorities (Article 39*quater* CCP), collection of identification data of electronic communications (Article 46*bis* CCP), cyber infiltration (Article 46*sexies* CCP), tracing of traffic data, and localization of electronic communications (Article 88*bis* CCP), and secret interception and secret (network) search (Article 90*ter* §1 CCP).

bb) Special investigation methods and any other methods of investigation

The Act of 6 January 2003 concerning special investigation methods and any other methods of investigation[3] introduced three special investigation methods and five other investigation methods into the CCP. Two of the other investigation methods are relevant for the interception of electronic communications: looking-in operations (Articles 46*quinquies* and 89*ter* CCP), and the power to enter a house or a private place to enable eavesdropping with technical means (former Article 90*ter* §1, 2° CCP). However, the latter provision was altered by the *Act of 25 December 2016 containing various amendments to the Code of Criminal Procedure and the Criminal Code, with a view to the improvement of the special investigation methods and certain investigation methods with respect to the internet and electronic and telecommunications and establishing a database of voice prints* ("Act of 25 December 2016").[4] The Act introduced the new term "interception" in Article 90*ter* CCP, a term which embodies both the general wiretapping measure (former Article 90*ter* §1, 1° CCP) and the measure to enter a house or a private place to enable eavesdropping with technical means (former Article 90*ter* §1, 2° CCP).

---

[2] The answers to the questions under this section are partially based on the first author's contribution to an EU-funded project on surveillance: Gertjan Boulet, "Regulating Surveillance: The Belgian case," Deliverable 2.3 (The Legal Perspective) for the EU-funded project Increasing Resilience in Surveillance Studies (IRISS), pp. 49–52, 31 January 2013, available at http://irissproject.eu/?page_id=9

[3] Act of 6 January 2003 concerning special investigation methods and any other methods of investigation, *Belgian Official Journal*, 12 May 2003, entry into force on 22 May 2003.

[4] Act of 25 December 2016 containing various amendments to the Code of Criminal Procedure and the Criminal Code, with a view to the improvement of the special investigation methods and certain investigation methods with respect to the internet and electronic and telecommunications and establishing a database of voice prints, *Belgian Official Journal*, 17 January 2017, entry into force on 27 January 2017.

cc) Cooperation with individuals and the private sector

For the execution of the above-mentioned investigation operations, Belgian law enforcement agencies can cooperate with individuals and the private sector (see section III.A.3.).

dd) Data retention

The general data retention provision is Article 126 of the Electronic Communications Act of 13 June 2005,[5] which addresses, among others, the providers that are subject to data retention obligations, the purposes of data retention, the obligations of the network and service providers, and the data retention periods. However, on 11 June 2015, the Belgian Constitutional Court invalidated Article 126 of the Electronic Communications Act. A new Belgian data retention Act of 29 May 2016 entered into force on 28 July 2016.[6]

A Royal Decree of 19 September 2013 lists the types of data subject to data retention.[7] Article 9 §7 of the Electronic Communications Act provides that a specific Royal Decree shall address the matter of data retention for providers of private electronic communications networks and electronic communications services that are not publicly available (closed groups of end-users). Considering the lack of such a Royal Decree, Federal Magistrate Jan Kerkhofs and Investigating Judge Philippe Van Linthout argue that Belgian private providers of electronic communications services or networks are currently released from data retention obligations.[8] For the same reason, the service providers that act as a mere conduit or provide caching and hosting activities under the Code of Economic Law are currently released from data retention obligations.

Legal experts[9] have mentioned the inapplicability of the general data retention legislation for GPS-data and bank accounts. No data retention law seems to govern the collection of GPS-data by Belgian law enforcement requests via car rental companies. However, the National Bank of Belgium, the Belgian Post Group (Bpost), credit institutions, investment companies, insurance companies, banks,

---

[5] As amended by the Belgian Communication Act of 30 July 2013 amending Articles 2, 126, and 145 of the Act of 13 June 2005 on electronic communications and Article 90*decies* CCP, *Belgian Official Journal*, 23 August 2013, entry into force on 2 September 2013.

[6] Act of 29 May 2016 on the collection and retention of data in the electronic communications sector, *Belgian Official Journal*, 18 July 2016, entry into force on 28 July 2016.

[7] Royal Decree of 19 September 2013 regarding the execution of Article 126 of the Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 8 October 2013, entry into force on 19 September 2013.

[8] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 396.

[9] The legal experts referred to in this report are the interviewed Federal Magistrates.

notaries, bailiffs, accountants (and others) are subject to specific (less strict) data retention and production obligations of the Act of 18 September 2017 on preventing misuse of the financial system for purposes of laundering money and terrorism financing.[10]

On 19 July 2018, the Constitutional Court of Belgium requested a preliminary ruling from the Court of Justice of the European Union (CJEU), regarding the compatibility of the Belgian general data retention obligation for traffic and localization data with EU law (see annex: explanatory note on legislative changes).[11]

b) Preventive law

The legal provisions for intercepting electronic communications under (preventive) police law are the general provision on crime detection and evidence gathering by the police (Article 8 CCP), and a specific provision on access by the police to publicly accessible places (Article 26 of the Act on the Police Function).[12] On 28 March 2017, the Belgian Supreme Court held that publicly accessible places in Article 26 of the Act on the Police Function also extends to publicly accessible places on the Internet, in casu when deepweb markets are accessible to the public via purely formal access procedures such as automatically generated invitation links.[13] Personalized access control procedures, on the other hand, such as personal invitations by existing members of the deepweb market, would render the deepweb market a "private place" (thus not accessible to the public).

Article 28*bis* §2 CCP, on proactive investigation, is the legal provision for intercepting electronic communications under (preventive) criminal law. Article 28*bis* §2 CCP explains that the proactive investigation falls under the preliminary investigation:[14]

> § 2. The preliminary investigation covers the proactive investigation. This is understood, in order to prosecute perpetrators of criminal offences, the detection, collection, registration and processing of data and intelligence on the basis of a reasonable suspicion of criminal offences to be committed or already committed but not yet exposed, and that

---

[10] Act of 18 September 2017 on preventing misuse of the financial system for purposes of laundering money and terrorism financing, *Belgian Official Journal*, 6 October 2017, entry into force on 16 October 2017. Article 60 of the Act provides a data retention period of 10 years, to be reduced to seven years in 2017, and to eight and nine years respectively in 2018 and 2019.

[11] Constitutional Court of Belgium, 19 July 2018, no. 96/2018, referring judgment of the Constitutional Court for preliminary rulings from the Court of Justice of the European Union (on the "collection and retention of data in the electronic communications sector"), available at http://www.const-court.be/public/n/2018/2018-096n.pdf

[12] Act of 5 August 1992 on the Police Function, *Belgian Official Journal*, 22 December 1992, entry into force on 1 March 1993.

[13] Supreme Court, 28 March 2017, AR P.16.1245.N, available via http://jure.juridat.just.fgov.be/

[14] All translations of statutory texts are the authors' own.

> are or would be committed in the context of a criminal organization as defined by law, or constitute or would constitute crimes or misdemeanours referred to in Article 90ter, §§ 2, 3 and 4. The initiation of a proactive investigation requires prior written permission by the public prosecutor, the labour prosecutor (or the federal prosecutor) in the context of their respective authority, without prejudice to compliance with the specific legal provisions governing special investigation methods and other methods.

The coercive powers of the home search, observation, entering private places in the context of a looking-in operation and the secret interception and secret (network) search cannot be used by the public prosecutor during the proactive investigation. This prohibition is based on an *a fortiori* reading of the legal basis for the mini-instruction (Article 28*septies* CCP), which is a legal notion allowing the public prosecutor, during the preliminary investigation phase, to request the investigating judge to perform investigative measures for which only the investigating judge is competent. However, the coercive powers of the home search, observation, entering private places in the context of a looking-in operation, and the secret interception and secret (network) search are excempted from the mini-instruction:

> The public prosecutor can request the investigating judge, without the initiation of a judicial investigation, to perform any investigation measure for which only the investigating judge is competent, with the exception of an arrest warrant referred to in Article 16 of the Act of 20 July 1990 on remand custody [pre-trial detention], the fully anonymous testimony referred to in Article 86bis, the monitoring measure referred to in Article 90ter [secret interception and secret (network) search], and the investigation measures referred to in Article 56bis, second paragraph [observation] and 89ter [looking-in operations, and network search during looking-in operations]. After the execution of the investigation measure carried out by the investigating judge, he shall decide whether to return the file to the public prosecutor who is responsible for the continuation of the investigation, or whether he will continue the whole investigation himself, in which case further action shall be taken in accordance with the provisions of Chapter VI of this book. There is no legal remedy against this decision.
>
> In case of a new request in the same file on the basis of the first paragraph, the case is brought before the same investigating judge if he is still in office.

In other words, Article 28*septies* CCP prohibits the public prosecutor, during the preliminary investigation phase (which, as noted, covers the proactive investigation), from requesting the investigating judge, without the initiation of a judicial investigation, to perform these coercive powers (for which only the investigating judge is competent).

Kennes (attorney-at-law) raises an additional argument against the use of coercive measures during the proactive investigation, by observing that, whereas the proactive investigation can be activated following a "reasonable presumption of punishable acts," the monitoring measure (Article 90*ter* CCP) is reserved for cases in which there are "serious indications that the offence is a criminal offence."[15] Van den Wyngaert, however, notes that the distinction between proactive and reactive

---

[15] Laurent Kennes, *Manuel de la preuve en matière pénale* (Manual on evidence in criminal matters), Mechelen, Kluwer, 2009, p. 209.

investigation is not always easy to draw, and that the European Court of Human Rights (ECtHR) in the case *Lüdi v. Switzerland*[16] held that a proactive wiretapping measure, if based on law, is not incompatible with the European Convention on Human Rights (ECHR).[17]

c) Law of intelligence agencies

The legal provisions for intercepting electronic communications under intelligence law are provided in the Act of 30 November 1998 on the Intelligence and Security Services.[18] Ordinary collection methods for State security include: intelligence collection with private actors (Article 16), the observation and search without technical means of public places (Article 16/1), and the request for identification data (Article 16/2).

Specific collection methods include: observation, with technical means, of publicly accessible places (Article 18/4); observation, with or without technical means, of private places that are not hidden from view (Article 18/4); search, with technical means, of publicly accessible places, and the content of objects (whether or not closed) that are available in publicly accessible places (Article 18/5); taking cognizance of the identification data of the sender or addressee of mail, or of the holder of a post-box (Article 18/6); requesting transport and travel data from any private provider of a transport or travel service (Article 18/6/1); collection of identification data of electronic communications (Article 18/7), the tracing of traffic data, and localization of electronic communications (Article 18/8).

Exceptional collection methods include: observation, with or without technical means, in private places that are hidden from view (Article 18/11), search, with or without technical means, of private places not accessible to the public (Article 18/12), using a legal person to collect data about events, objects, groups and natural or legal persons that are relevant for the exercise of their functions (Article 18/13), the collection of data regarding bank accounts and banking operations (Article 18/15), intrusion into a computer system, with or without technical means, false signals, false keys or false identities (Article 18/16), and intercepting, taking cognizance of and recording of communication (Article 18/17). For the execution of the above-mentioned intelligence operations, Belgian intelligence agencies can cooperate with individuals and the private sector (Article 16, Article 16/2, Article 18/6,

---

[16] ECtHR, *Lüdi v. Switzerland*, 15 June 1992, Grand Chamber, no. 12433/86, available via http://hudoc.echr.coe.int/

[17] Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, pp. 683, 843, 986, footnote 4399.

[18] Act of 30 November 1998 Law on the Intelligence and Security Services, *Belgian Official Journal*, 18 December 1998, entry into force on 1 February 1999.

Article 18/6/1, Article 18/7, Article 18/8, Article 18/16, Article 18/17 of the Act of 30 November 1998 on the Intelligence and Security Services).

Regarding the powers of the (military) General Intelligence and Security Service of the Armed Forces (GISS), Article 44 of the Act of 30 November 1998 provides the power for GISS to detect, intercept, eavesdrop, to take cognizance of and record any form of communications transmitted or received abroad.

Article 44/5 of the Act of 30 November 1998 empowers the GISS, if an intervention on a communications network is necessary to enable the interception of communication transmitted or received abroad as referred to in Article 44, to request the operator of the communications network or the provider of the electronic communications service to provide his cooperation as soon as possible. Anyone who refuses to cooperate with this request shall be punished by a fine of 26 euros to 20,000 euros.

Article 44/1 of the Act of 30 November 1998 empowers the GISS to proceed with the intrusion into a computer system that is located abroad, suspend its security, install technical equipment in the system in order to decipher, decode, save and manipulate the data stored, processed or forwarded by the computer system, and to disrupt and neutralize the computer system.

d) Customs Investigation Service

Belgian law does not grant powers to Belgian Customs Investigation Services to intercept electronic communication. Cybersquad, falling under the investigation services of the General Administration Customs and Excise (Federal Public Service Finance),[19] has powers, among others, to block websites offering illegal goods. The Belgian Internet Service Center (BISC), established in 2011 under the Special Tax Inspectorate of the Federal Public Service Finance,[20] has powers to investigate Internet fraud: it detects infringements of Belgian law by online shops offering goods in Belgium and controls domain names with the extension ".be." BISC also has software to map suspicious websites.[21]

---

[19] Federale Overheidsdienst Financiën, Algemene Administratie der douane en accijnzen (in Dutch), Service Public Fédéral Finances, Administration générale des douanes et accises (in French).

[20] Bijzondere Belastinginspectie (BBI, in Dutch), Inspection spéciale des impôts (ISI, in French).

[21] Christina Bourlet, "La lutte contre la fraude de mass: développements récents" (the fight against mass fraud: recent developments), in Dominique Grisay (ed.), *De la lutte contre la fraude à l'argent du crime: État des lieux*, Brussels, Groupe De Boeck, 2013, pp. 83–98.

3. Responsibility for the technical performance of interception measures

a) Material competence

The responsibility for the technical performance of interception measures under police law lies with the judicial police.

The responsibility for the technical performance of interception measures under (preventive) criminal law lies with the public prosecutor.

The responsibility for the technical performance of interception measures under (reactive) criminal law lies with the investigating judge, the public prosecutor, and judicial police officers.

The responsibility for the technical performance of interception measures under intelligence law lies with both the Director-General of the intelligence and security agencies and the administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services (SIM commission).

b) Territorial competence

The police and law enforcement agencies are structured at the federal and local levels. The intelligence agencies are structured at the federal level. There is one federal public prosecutor. The local public prosecutor's offices are situated at the same level as the Courts of First Instance: the judicial districts (Article 150 §1 Judicial Code). The 2014 judicial reform reduced the judicial arrondissements (districts) from 27 to 12, of which the boundaries overlap with nine of the 10 provinces (West Flanders, East Flanders, Antwerp, Limburg, Hainaut, Namur, Walloon Brabant, Liège, Luxembourg) and the cities Leuven (province Flemish Brabant), Brussels (province Flemish Brabant), and Eupen for German-speaking Belgium (part of the province Liège).[22]

The Act of 19 July 2012 on the reform of the judicial arrondissement Brussels[23] split up the public prosecutor's office covering the area Brussels-Halle-Vilvoorde (Article 152 §2 Judicial Code). The Act of 19 July 2012 created, on the one hand, a public prosecutor's office covering the administrative arrondissement of Brussels-Capital and, on the other hand, a public prosecutor's office covering the administrative arrondissement Halle-Vilvoorde. In other words, a public prosecutor's office

---

[22] The rationale behind the division into 27 districts, dating back to the foundation of Belgium in 1831, is to reach every capital city in each district by horse in one day. On the judicial reform in Belgium, see Stefaan Voet, "Belgium's new specialized judiciary," *Russian Law Journal*, 2014, vol. II, issue 4, pp. (129) 130, 138.

[23] Act of 19 July 2012 on the reform of the judicial district Brussels, *Belgian Official Journal*, 22 August 2012, entry into force on 31 March 2014.

was created for the administrative district of Brussels-Capital, which covers the bilingual (French and Dutch) 19 municipalities of the Brussels-Capital Region (better known as Brussels); another public prosecutor's office was created for the administrative district Halle-Vilvoorde, which surrounds Brussels and consists of 35 Dutch-speaking municipalities, including 6 municipalities with language facilities for French-speakers.

The local Prosecutor General's offices are situated at the level of the courts of appeal (Article 143 §1 Judicial Code), more particularly in the five judicial areas (Ghent, Brussels, Antwerp, Mons, Liège).

At the federal level, there is a Prosecutor General's office at the Supreme Court (Article 142 Judicial Code), and a Federal Prosecutor's office that is competent for the whole territory of Belgium (Article 143 §1 Judicial Code).

The investigating judges are situated at the Courts of First Instance and are appointed by the King from among the judges at the Courts of First Instance (Article 58*bis*, 4° Judicial Code and Article 259*sexies* 1° Judicial Code).

c) Cooperation with individuals and the private sector

As mentioned above (section I.A.2.), for the execution of investigation and intelligence operations, Belgian law enforcement agencies and intelligence agencies can cooperate with individuals and the private sector.

4. Legitimacy of data transfers between different security agencies

There is a separation between the various institutions responsible for the interception of electronic communication under the police law, criminal law, and intelligence law. Thus, there are no joint agencies that carry out interception.

However, the results of interception measures under these different legal regimes can be exchanged between the competent authorities.

a) Exchange of data between law enforcement authorities and preventive police authorities

Article 15, 1° of the Act of 5 August 1992 on the Police Function reads as follows:

> In the performance of their judicial police functions, the police services have the task:
>
> 1° to detect the crimes, misdemeanours and contraventions, to gather evidence thereof, to notify the competent authorities thereof, to apprehend, the perpetrators, to arrest them, and to bring them at the disposal of the competent authorities, in the manner and forms provided by law; […]

There are several provisions that imply data exchanges from police authorities to law enforcement authorities.

– Article 28*bis* §1 CCP provides that preliminary investigations are conducted under the direction and authority of the competent public prosecutor. This is confirmed by Article 6 of the Act of 5 August 1992 on the Police Function.
– Article 29 CCP provides that any authority shall immediately inform the public prosecutor of a crime or misdemeanour that comes to its knowledge. Article 44/1 §3 of the Act of 5 August 1992 on the Police Function provides that police authorities, in the exercise of their administrative police functions, shall immediately inform the competent judicial authorities of personal data and information that is important for the exercise of the judicial police functions.
– Article 53 CCP provides that the judicial police officers shall immediately send the reports (of an offence), official records,[24] and any other acts drafted under their competence to the public prosecutor. This provision is echoed by Article 40 of the Act of 5 August 1992 on the Police Function, which provides that police officers shall send official records on complaints, reports of offences, intelligence, and any detections to the competent judicial authorities.
– Article 54 CCP provides that the judicial police officers shall immediately send any reports of crimes and misdemeanours they are not competent to detect to the public prosecutor.
– Article 5/3 of Act of 5 August 1992 on the Police Function provides that, for the performance of judicial police functions, the police shall maintain regular service relations with the local public prosecutors, the federal public prosecutor, and the Prosecutors General.

In principle, the police authorities do not forward simplified official records, which are used for relatively non-serious offences,[25] to the public prosecutor. The police authorities only send a monthly list to the public prosecutor, which contains the number of the simplified official records; a short description of the offence; the qualification, place, and time of the offence; and the identity of the implicated persons. The circular of 15 June 2005 issued by the Board of Prosecutors General lays down the rules on simplified official records.[26]

The project "Autonomic Police Treatment" (APT)[27] allows for independent police treatment in specific cases. Article 28*bis* §1, 2° CCP provides that the law and special rules issued via circular by the Board of Prosecutors General[28] determine

---

[24] *Proces-verbaal* (in Dutch), *procès-verbal* (in French).

[25] *Vereenvoudigd proces-verbaal* (in Dutch), *procès-verbal simplifié* (in French).

[26] Board of Prosecutors General, Circular of 15 June 2005, COL 8, available (in Dutch and French) at https://www.om-mp.be/

[27] Previously called *Autonome Politionele Afhandeling* (APA, in Dutch), or le *Traitement Policier Autonome* (in French); currently called *Ambtshalve Politioneel Onderzoek* (APO, in Dutch), or *Enquête Policière d'Office* (in French).

[28] The Board of Prosecutors General (*College van procureurs-generaal* in Dutch; *Collège des procureurs généraux* in French) can take measures to ensure a coherent im-

the general principles for APT. The circular of 15 June 2005 issued by the Board of Prosecutors General lays down the rules on APT.[29] Research on APT explains that APT "breaks with the tradition of the public prosecutor as a mere sender and receiver of instructions (a 'letter-box'); all necessary police research should be finished before the file can be sent to the public prosecutor's office."[30] The research finds that APT is a "manner" for the public prosecutor to realize investigation policy, on the basis of Article 28*ter* §2 CCP, which provides that judicial police officers and agents acting on their own initiative shall inform the public prosecutor of the conducted investigations within the time and in the manner provided by the public prosecutor in a directive (circular). In a judgment of 21 August 2001, the Supreme Court confirmed the possibility of APT without prior notification of the public prosecutor.[31] The Supreme Court also held that the notification duty laid down in Article 28*ter* CCP is not substantial and not prescribed under penalty of nullity.

b) Passing on of data by intelligence agencies

Regarding information transfers from the intelligence and security services to the police services, Article 20 §1 of the Act of 30 November 1998 on the Intelligence and Security Services lays down a general obligation of efficient mutual cooperation between intelligence and security services, police services, administrative and judicial authorities, as well as with foreign intelligence and services.

Furthermore, the Act of 18 March 2014 inserted a new Article 44/11/9 into the Act of 5 August 1992 on the Police Function, §4 of which lays down a duty for the intelligence and security services and other services to transfer data and information, which are processed in the context of their functions and that are sufficient, relevant, and not excessive in view of police functions, to the police services.

Regarding information transfers from the intelligence and security services to the judicial authorities, there are three ways to transfer information:

---

plementation and coordination of criminal policy laid down in ministerial directives and the good general and coordinated functioning of the public prosecutor's office (Article 143*bis* §2 Judicial Code).

[29] Board of Prosecutors General, Circular of 15 June 2005 regarding the Autonomic Police Treatment and the simplified official records, COL 8, available (in Dutch and French) at http://www.om-mp.be/omzendbrief/4016820/omzendbrief_col_8_d_d__15_06_2005.html. The circular also lays down the rules on the simplified official record (see above under this section).

[30] An English summary of the APT project "Policing: Relative Autonomy? An empirical research into Autonomic Police Action" is available at http://www.belspo.be/belspo/organisation/publ/pub_ostc/SoCoh/rSO02016_en.pdf

[31] Supreme Court, 21 August 2011, P.01.1203.F/1, available via http://jure.juridat.just.fgov.be/

First, Article 20 §1 of the Act of 30 November 1998 on the Intelligence and Security Services lays down a general obligation of efficient mutual cooperation between intelligence and security services, police services, and administrative and judicial authorities. Article 20 §2 of the Act of 30 November 1998 on the Intelligence and Security Services provides that the intelligence and security services can cooperate with the judicial and administrative authorities, upon their request, and within the limits of a protocol adopted by the relevant ministers.

Article 19 provides that the intelligence and security services shall only transfer intelligence to the concerned ministers or judicial and administrative authorities, the police services, and all competent organizations and persons according to the purposes of their functions and in relation to threatened organizations and persons.

A service note of the Federal Prosecutor of 17 December 2012 on the written information exchanges between the intelligence and security services and the public prosecutor is based on the unpublished circular COL 9/2012 of 21 June 2012 of the Board of Prosecutors General regarding the Act of 30 November 1998 on the Intelligence and Security Services; it determines the principles regarding the use and preservation of classified information at the federal public prosecutor's office.[32]

For the data transfer from intelligence agencies to judicial authorities, there is no similar provision to Article 14 §1-2 of the Act of 30 November 1998 on the Intelligence and Security Services, which allows information transfers from judicial authorities and police services, on their own initiative, to intelligence and security services (see I.A.4.c. below).

Second, Article 19/1 §1 of the Act of 30 November 1998 on the Intelligence and Security Services provides that, in view of the application of Article 29 CCP,[33] these services shall immediately inform the administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services (SIM commission) if the performance of specific or exceptional collection methods reveals serious indications of the commission of a crime or misdemeanor, or, in case of reasonable suspicion, of unrevealed or future offences.

Article 19/1 §2 of the Act of 30 November 1998 on the Intelligence and Security Services provides that, if the SIM commission confirms the findings of the intelligence and security services, then the president of the SIM commission shall draft an unclassified official record and immediately send it to the public prosecutor or

---

[32] Federal Prosecutor's Office, Annual report of the Public Prosecutor's Office to the Board of Prosecutors General for the period 1 January 2012 till 23 December 2012, 2012, p. 124, available (in Dutch) at https://www.om-mp.be/

[33] Article 29 CCP provides that any authority shall immediately inform the public prosecutor of a crime or misdemeanor that comes to its knowledge (see section I.A.4.a.). This article also applies to the intelligence and security services.

the federal prosecutor after having heard the Director-General of the intelligence and security agencies regarding the transfer conditions.

Third, there is an additional information flow from the oversight body of the intelligence agencies, i.e., the Belgian Standing Intelligence Agencies Review Committee (Standing Committee I), to the judicial authorities. The Standing Committee I acts as a prejudicial advisor if the Council Chamber[34] (Article 131*bis* CCP) or the court dealing with the substance of the case (Article 189*quater* CCP) or the Court of Assize (Article 279*bis* CCP), when confronted with an unclassified official record as referred to in Article 19/1 of the Act of 30 November 1998 on the Intelligence and Security Services, requests the advice of the Standing Committee I on the legality of the collection methods used by the intelligence services.

c) Passing on of data to intelligence agencies

Regarding the transfer of information from the police services and judicial authorities to the intelligence and security services, first, Article 20 §1 of the Act of 30 November 1998 on the Intelligence and Security Services lays down a general obligation of maximum efficient mutual cooperation between intelligence and security services, police services, and administrative and judicial authorities.

Second, Article 14 §1-2 of the Act of 30 November 1998 on the Intelligence and Security Services provides that the civil servants and agents of public services (including police services) and judicial authorities, can transfer information that is useful for the functions of the intelligence and security services, on their own initiative or upon request. Article 14 §2 of the Act of 30 November 1998 on the Intelligence and Security Services provides that the civil servants and agents of public services (including police services) and judicial authorities can refuse to transfer information, if they deem that such a transfer would compromise an ongoing (preliminary) investigation or the collection of information according to the Act of 11 January 1993 on preventing misuse of the financial system for purposes of laundering money and terrorism financing, or if it could harm someone in his or her personal physical integrity.

---

[34] The Council Chamber (*Raadkamer* in Dutch; *Chambre du conseil* in French) supervises the investigation phase at the Court of First Instance. The Indictment Chamber or Court of Indictment (*Kamer van Inbeschuldigingstelling* in Dutch; *Chambre des mises en accusation* in French) supervises the investigation phase at the Court of Appeal.

B. Statistics on Telecommunications Interception

1. Obligation to collect statistics

Law enforcement authorities and courts are obliged to report statistics to the Ministry of Justice. Article 90*decies* CCP provides that the Minister of Justice will report annually to the Parliament on the application of some but not all investigation methods:

> The Minister of Justice reports every year to Parliament on the application of Articles 90ter to 90novies [secret interception and secret (network) search].
>
> He shall inform the Parliament of the number of investigations that gave rise to the measures referred to in those articles, the duration of those measures, the number of persons involved and the results obtained.
>
> He also reports at the same time on the application of Articles 40bis [the authorization by the prosecutor of the police services to postpone the apprehension of the suspected perpetrators of crimes and the seizure], 46ter [the interception and opening of classical mail], 46quater [the collection of data regarding bank accounts and bank transactions], 46quinquies [looking-in operations], 47ter to 47decies [observation, infiltration, citizen infiltration and the use of informants], 56bis [special investigation methods targetet at lawyer or doctor], 86bis [anonymous testimonials], 86ter [documentation requirements regarding anonymous testimonials], 88sexies [opening of intercepted or seized post on the basis of Article 46ter CCP], and 89ter [network search during looking-in operations].
>
> He informs Parliament of the number of investigations that gave rise to the measures referred to in these articles, the number of persons involved, the crimes to which they related and the results obtained. […]

The annual reports of the Minister of Justice in implementation of Article 90*decies* CCP[35] provide that data collection and processing is determined via the confidential circular COL 17/2006 of the Board of Prosecutors General. The annual reports of the Minister of Justice in implementation of Article 90*decies* CCP give some explanations about the information providers and the data collection procedure.

Regarding the information providers, the federal police provides data regarding the power to enter a house or a private place in order to enable eavesdropping with technical means and looking-in operations; the National Informants Administrator, which functions at the judicial police's Directorate-General level under the supervision of the federal prosecutor (Article 47*decies* §2 CCP),[36] provides data on informants; the investigating judge (via the public prosecutors) provides data on anonymous witnesses and other investigation methods; the federal prosecutor provides data on anonymous witnesses, the protection of threatened witnesses, special investigation methods, and the other investigation methods.

---

[35] The reports in implementation of Article 90*decies* CCP are available at the website of the Criminal Policy Service of the Ministry of Justice: http://www.dsb-spc.be/

[36] *Nationale Informantenbeerder* (in Dutch), *Gestionnaire des indicateurs* (in French).

The annual reports add that all information, except information regarding the interception method (Article 90*ter* CCP), is provided via uniform forms and sent to the Criminal Policy Service of the Ministry of Justice.[37] For information regarding the interception methods, the reports mention two ways of data gathering: first, an automatic transfer for users of the programme "Phoobs."[38] Phoobs was developed by the federal police to standardize data collection with the different operators. Phoobs creates an access file which is sent to the Federal Computer Crime Unit (FCCU) of the Federal Judicial Police (Directorate for Combating Economic and Financial Crime). Second, for non-Phoobs users, the FCCU requires completion of an Excel spreadsheet by the investigating judge. The annual reports add that the FCCU also receives data from the federal police's unit that technically implements the interception measure: the "Commissariat-general Special Units – National Technical and Tactical Support Unit – Central Technical Interception Facilities."

The Criminal Policy Service of the Ministry of Justice processes the data and drafts the report for the Minister of Justice, with the Board of Prosecutors General in copy.

2. Current data

This section shows current data for law enforcement methods, intelligence collection methods and government access. This data is provided by, respectively, the Ministry of Justice, the Belgian Standing Intelligence Agencies Review Committee (Standing Committee I), and Internet service providers.

a) Current data for law enforcement methods provided by the Ministry of Justice

aa) Overview

As stated above (section I.B.1.), the Minister of Justice will report annually to the Parliament on the application of some but not all investigation methods. Article 90*decies* CCP requires reporting for only two electronic communications interception methods: the network search during looking-in operations (Article 89*ter* CCP), and the secret interception and secret (network) search (Article 90*ter* CCP). Hence, there are no reporting obligations for the data seizure and non-secret (net-

---

[37] *Dienst voor het Strafrechtelijk Beleid* (in Dutch), *Service de la Politique Criminelle* (in French).

[38] Belgian Institute for Postal Services and Telecommunications, "Synthese van de raadpleging door de raad van het bipt op verzoek van de minister voor ondernemen en vereenvoudigen van 29/04/2010 betreffende de praktische uitvoering van richtlijn 2006/24/EG van 15 maart 2006 (richtlijn betreffende de bewaring van gegevens)" (Summary regarding the implementation of the data retention directive 2006/24/EG of 15 March 2006), 2010, p. 14, available at http://www.bipt.be/public/files/nl/1259/3344_nl_2010-10-01_bipt-verslag_consultatie_data_retention-publieke_versie_v20101001_nl.pdf

work) search (Article 39*bis* CCP), the collection of identification data of electronic communications (Article 46*bis* CCP), cyber infiltration (Article 46*sexies* CCP), and tracing of traffic data, and localization of electronic communications (Article 88*bis* CCP). The annual reports of the Minister of Justice in implementation of Article 90*decies* CCP do not specify the cases in which the special investigation methods (which are subject to the reporting obligation) were used in the context of the interception of electronic communication.

The annual reports of the Minister of Justice in implementation of Article 90*decies* CCP mention productive cooperation with the federal public prosecutor's office and the federal police, which resulted in accurate statistics on looking-in operations and the special investigation methods. But for the other investigation methods, the annual reports mention incomplete data collection and lacking coordination between the investigating judges and the public prosecutors. The annual reports therefore refer to term indications instead of statistics. Furthermore, on the interception measure, the annual reports mention the lack of general cooperation between the federal judicial police and local police services, such as failing to complete the evaluation forms and return them to the Ministry of Justice.

bb) Wiretapping

As stated above (section I.A.2.a.bb.), the Act of 25 December 2016 introduced the new term "interception" in Article 90*ter* CCP, which embodies both the general wiretapping measure (former Article 90*ter* §1, 1° CCP) and the measure to enter a house or a private place to enable eavesdropping with technical means (former Article 90*ter* §1, 2° CCP).[39] Hence, the annual reports before 2016 provide data for both the wiretapping measure and the eavesdropping measure. However, there are no published annual reports after 2013.

The first table below this section gives an overview of the number of wiretapping measures performed by law enforcement agencies (Article 90*ter* §1, 1° CCP). The table also sorts these numbers according to the object of the wiretapping measures.

The 2004 annual report provides numbers in relation to the following categories of telecommunications: 117 wiretaps of landline numbers; 1390 wiretaps of mobile numbers; 9 wiretaps of fax numbers; 5 wiretaps of the Internet (modems); and 136 non-specified wiretaps. Regarding the eavesdropping measure, the 2004 annual report indicates that only one public prosecutor's office provided data (two cases of eavesdropping). The 2005 annual report, however, provides more specific data on eavesdropping for 2004: 38 cases.

---

[39] See section 1.A.2.bb.: the Act of 25 December 2016 introduced the new term "interception" in Article 90*ter* CCP, a term which embodies both the general wiretapping measure (former Article 90*ter* §1, 1° CCP) and the measure to enter a house or a private place to enable eavesdropping with technical means (former Article 90*ter* §1, 2° CCP).

Since 2005, the annual reports have used different categories of telecommunications: landline numbers, mobile numbers, IMEI numbers, and emails. The 2011, 2012, and 2013 reports (for the years 2010, 2011 and 2012, respectively) present a non-numerical marked line chart. The numbers provided below are an estimate based on the author's reading of these charts.

Wiretapping (Article 90*ter* §1, 1° CCP)					
Year	Number (#)	Object (#, estimate)			
		Landline	GSM	IMEI	Mail
2005	2569	373	1660	536	0
2006	3036	511	2089	436	0
2007	3603	495	2473	632	3
2008	4881	686	3133	1062	0
2009[40]	5653	114	2818	531	3
2010	6031	631 (estimate)	4200 (estimate)	1200 (estimate)	0
2011	6671	621 (estimate)	4800 (estimate)	1250 (estimate)	0
2012	6712	712 (estimate)	4700 (estimate)	1300 (estimate)	0

cc) Power to enter a house or a private place to enable eavesdropping with technical means

The second table concerns the power to enter a house or a private place in order to enable eavesdropping with technical means performed by law enforcement agencies (Article 90*ter* §1, 2° CCP): the reports of the Ministry of Justice do not indicate the number of measures executed but only the annual number of case files in which the measures were applied.

Power to enter a house or a private place to enable eavesdropping with technical means (Article 90*ter* §1, 2° CCP)	
Year	Number of case files in which measure applied (#)
2004	38
2005	29
2006	24

[40] The annual report of 2010 provides a total number of wiretaps in 2009, which exceeds the sum of the numbers provided per category in the same report.

Power to enter a house or a private place to enable eavesdropping with technical means (Article 90*ter* §1, 2° CCP)	
Year	**Number of case files in which measure applied (#)**
2007	24
2008	40
2009	40
2010	48
2011	54
2012	71

b) Current data for intelligence collection methods provided by the Belgian Standing Intelligence Agencies Review Committee (Standing Committee I)

aa) Overview

The next few tables show the number of authorizations granted by the two intelligence agencies for the interception of electronic communication. The data is found in the activity reports of the Belgian Standing Intelligence Agencies Review Committee (Standing Committee I),[41] which has provided data on the specific collection methods since 2010 and on the exceptional collection methods since 2011. Thus, contrary to the lack of reporting obligations for law enforcement authorities regarding electronic communication interception methods other than the network search during looking-in operations (Article 89*ter* CCP) and the secret interception and secret (network) search (Article 90*ter* CCP), the Standing Committee I provides statistics on *all* electronic communication interception methods.

The relevant specific collection methods are the collection of identification data of electronic communications (Article 18/7 of the Act of 30 November 1998), the tracing of traffic data, and the localization of electronic communications (Article 18/8 of the Act of 30 November 1998).

The relevant exceptional collection methods are the intrusion into a computer system (Article 18/16 of the Act of 30 November 1998) and wiretapping (Article 18/17 of the Act of 30 November 1998).

Of note is that the Standing Committee I did not provide any statistics regarding the interception of communication transmitted from abroad by the General Intelligence and Security Service of the Armed Forces (GISS) (Article 44*bis* of the Act of 30 November 1998).

---

[41] Belgian Standing Intelligence Agencies Review Committee (Standing Committee I), "Activity reports," available (in Dutch and French) at http://www.comiteri.be/. The activity reports since 2006 are available in English.

We only provide statistics that exclusively address the interception of electronic communication. The reason is, again, the lack of specification regarding cases in which other law enforcement measures (not explicitly created for the interception of electronic communication) were used for the interception of electronic communication.

The Standing Committee I provides separate statistics for the (civil) State Security[42] and the (military) General Intelligence and Security Service of the Armed Forces (GISS).[43] The 2010 activity report notes that the Standing Committee I could not give an indication of the number of measures actually implemented by the State Security, as the latter used its legal power to send these listings to the SIM commission only. The GISS, however, gave an indication of the results delivered by the various methods and, even more, showed the lack of implementation of a large number of methods authorized by the GISS in the reference period.[44]

bb) Collection of identification data of electronic communications

The first table below refers to the specific collection method of collecting identification data of electronic communications (Article 18/7 of the Act of 30 November 1998). Of note is that, before 2013, the Standing Committee I did not show the number of measures but the annual number of case files in which these measures were applied.

In the 2012 activity report, the Standing Committee I explains that the decreasing frequency of both the collection of identification data of electronic communications and of tracing traffic data of electronic communications resulted from its decision that the authorization for these measures could no longer be used to also collect localization data.[45] In the 2013 activity report, the Standing Committee I confirmed an increasing number of localizations of electronic communications by both the State Security and the GISS.[46]

Since January 2013, the collection of identification data can no longer be authorized by the same authorization for the tracing of traffic data.[47] The collection

---

[42] *De Veiligheid van de Staat* (VSSE, in Dutch), *La Sûreté de l'Etat* (VSSE, in French).

[43] *De Algemene Dienst Inlichtingen en Veiligheid* (ADIV, in Dutch), le *Service général du Renseignement et de la Sécurité* (SGRS, in French).

[44] See the 2010-2011 activity report (in English), pp. 68–69.

[45] See the 2012 activity report of the Standing Committee I, p. 49.

[46] See the 2013 activity report of the Standing Committee I, p. 69 (footnote 129), p. 71 (footnote 135), and p. 72.

[47] See the English 2010–2011 activity report of the Standing Committee I, p. 148; the 2012 activity report of the Standing Committee I, p. 49; and the 2013 activity report of the Standing Committee I, p. 68.

of identification data stagnated in the same year, but almost doubled in 2014 and 2015.

Collection of identification data of electronic communications (Article 18/7 Act of 30 November 1998)		
Year	Before 2013: number of case files in which measure applied (#) Since 2013: number of measures (#)	
	State Security	GISS
2010	15 case files	8 case files
2011	355 case files	23 case files
2012	254 case files	25 case files
2013	243 case files 613 measures	16 case files 66 measures
2014	554 measures	67 measures
2015	663 measures	55 measures

cc) Tracing of traffic data, and localization of electronic communications

The next table concerns the specific collection method of tracing of traffic data of electronic communications, and localization of electronic communications (Article 18/8 of the Act of 30 November 1998).

Tracing of traffic data, and localization of electronic communications (Article 18/8 Act of 30 November 1998)				
Year	Tracing of traffic data (#)		Localization (#)	
	State Security	GISS	State Security	GISS
2010	30	7	6	7
2011	237	17	46	13
2012	147	30	176	4
2013	136	15	244	36
2014	88	12	248	28
2015	33	12	361	16

dd) Intrusion into a computer system

The next table concerns the specific collection method of intrusion into a computer system.

Intrusion into a computer system (Article 18/16 Act of 30 November 1998)		
Year	Number (#)	
	State Security	GISS
2011	3	0
2012	10	2
2013	12	0
2014	18	3
2015	16	3

ee) Wiretapping

In the 2013 activity report, the Standing Committee I refers to an increasing number of wiretapping measures by both the State Security and GISS.[48] The increase of wiretapping measures after 2013 is less pronounced.

Wiretapping (Article 18/17 Act of 30 November 1998)		
Year	Number (#)	
	State Security	GISS
2011	11	2
2012	50	14
2013	81	17
2014	86	26
2015	87	25

c) Current data provided by electronic communication companies

aa) Vodafone

The 2014 law enforcement disclosure report of the telecommunications company Vodafone includes a legal annex with an overview of law enforcement and intelligence powers in several countries, including Belgium.[49] Vodafone refers to two demands for disclosure of communication data by Belgium, and mentions that because Vodafone did not implement the technical requirements necessary to enable

[48] See the 2013 activity report, p. 72.

[49] Vodafone, "Law Enforcement Disclosure Report," 2014, available at http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

lawful interception, it did not receive any agency or authority demands for lawful interception assistance.[50] The 2015-16 law enforcement assistance report of Vodafone refers to zero demands for disclosure of communication data.[51]

bb) Google

The following table shows the number of requests for user data that the technology company Google received, the number of users/accounts specified in these requests, and the percentage of requests that Google complied with.[52]

User data requests to Google			
Period	**Number (#)**	**Users/accounts (#)**	**Compliance rate (%)**
July to December 2009	67	No data provided	No data provided
January to June 2010	71	No data provided	No data provided
July to December 2010	85	No data provided	73 %
January to June 2011	90	111	67 %
July to December 2011	99	124	67 %
January to June 2012	107	127	67 %
July to December 2012	120	153	63 %
January to June 2013	194	289	66 %
July to December 2013	162	206	73 %
January to June 2014	213	513	73 %
July to December 2014	214	297	67 %
January to June 2015	243	311	71 %
July to December 2015	268	350	72 %
January to June 2016	248	326	72 %
July to December 2016	259	304	71 %

[50] *Ibid.*, p. 71; see also Vodafone's "country-by-country disclosure of law enforcement assistance demands," available at http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html

[51] Vodafone, "Country-by-Country Disclosure of Law Enforcement Assistance Demands 2015-16," 2015, available at https://www.vodafone.com/content/dam/vodafone-images/sustainability/drf/pdf/vodafone_drf_law_enforcement_disclosure_country_demands_2015-6.pdf

[52] Google Transparency Reports, available via http://www.google.com/transparencyreport/?hl=en_US

User data requests to Google			
Period	**Number (#)**	**Users/accounts (#)**	**Compliance rate (%)**
January to June 2017	279	349	72 %
July to December 2017	320	389	74 %

cc) Microsoft

The following table shows the number of law enforcement requests addressed to the technology company Microsoft.[53] Like Google, Microsoft provides the number of requests for user data it has received, the number of users/accounts specified in these requests, and the percentage of requests it complied with. Unlike Google's transparency reports, Microsoft breaks the compliance rate into three percentages: provided subscriber/transactional data; provided content data; or no data provided because no data was found. In addition, Microsoft provides a rejection rate showing the percentage of rejected requests for failure to meet legal requirements. The law enforcement request reports cover requests for all Microsoft services, except for the 2012 report, which does not cover the voice-call service Skype.

User data requests to Microsoft						
Period	**Number (#)**	**Rejection rate (#, %)**	**Users/ accounts (#)**	**Non-content data (#, %)**	**Content data (#, %)**	**No data found (#, %)**
January to December 2012	727	0 %	1140	629 86.5 %	0 %	98 13.5 %
January to June 2013	500	0 %	784	406 81.2 %	0 %	94 18.8 %
July to December 2013	378	12 3.2 %	520	287 75.9 %	0 %	79 20.9 %
January to June 2014	433	66 1 %	922	360 83.1 %	0 %	66 15.2 %
July to December 2014	481	17 3.5 %	765	394 81.9 %	0 %	70 14.6 %
January to June 2015	406	34 8.37 %	600	297 73.16 %	0 %	75 18.47 %
July to December 2015	481	54 11.23 %	852	359 74.64 %	0 %	68 14.14 %

[53] Microsoft Law Enforcement Requests Reports, available via https://www.microsoft.com/en-us/about/corporate-responsibility/lerr

User data requests to Microsoft						
Period	**Number (#)**	**Rejection rate (#, %)**	**Users/ accounts (#)**	**Non-content data (#, %)**	**Content data (#, %)**	**No data found (#, %)**
January to June 2016	351	43 12.25 %	453	251 71.51 %	0 %	57 16.24 %
July to December 2016	357	23 6.44 %	456	281 78.71 %	0 %	53 14.85 %
January to June 2017	329	27 8.21 %	441	252 76.60 %	0 %	50 15.20 %
July to December 2017	267	20 7 %	472	205 77 %	0 %	42 16 %

dd) Twitter

The transparency reports of the social networking service provider Twitter show an increase of information requests from zero in 2012 to 25 in 2017.[54]

User data requests to Twitter			
Period	**Account information requests (#)**	**Compliance (%)**	**Accounts (#)**
January to June 2012	No data provided	No data provided	No data provided
July to December 2012	0	Not applicable	Not applicable
January to June 2013	0	Not applicable	Not applicable
July to December 2013	2	50 %	2
January to June 2014	0	Not applicable	Not applicable
July to December 2014	1	0 %	1
January to June 2015	5	40 %	7
July to December 2015	11	82 %	11
January to June 2016	67	88 %	75
July to December 2016	21	48 %	72
January to June 2017	21	67 %	32
July to December 2017	25	64 %	34

[54] Twitter Transparency reports, available via https://transparency.twitter.com/

ee) Facebook

The government request reports of the social media service provider Facebook show an increasing number of requests (like Google).[55] Whereas Google's compliance rate has remained stable at around 70 %, Facebook's compliance rate gradually decreased until June 2015, but increased to almost 90 % in December 2017.

Facebook's transparency reports since 2016 break the requests rates into two percentages: legal process and emergency requests.

User data requests to Facebook			
Period	**Number (#)**	**Compliance (%)**	**Users/accounts (#)**
January to June 2013	150	70 %	169
July to December 2013	154	64.94 %	196
January to June 2014	209	56.94 %	246
July to December 2014	239	59 %	319
January to June 2015	281	68.68 %	356
July to December 2015	290	77.24 %	375
January to June 2016	420 (397 legal process; 23 emergency requests)	86.43 %	674
July to December 2016	399 (379 legal process; 20 emergency requests)	85.46 %	682
January to June 2017	513 (486 legal process; 27 emergency requests)	85 %	757
July to December 2017	552 (531 legal process; 21 emergency requests)	87 %	803

ff) Verizon

The transparency reports of the US telecommunications provider Verizon do not show the total number of requests received, nor compliance or rejection rates.[56]

Until the report for the second half of 2014, the transparency reports did not provide statistics on requests for subscriber information and transactional information.

The 2013 transparency report specifies customer selectors (number of users/accounts specified in the requests) for all requests complied with. The transparency report since the first half of 2014 breaks the customer selector rates into numbers for subscriber information and transactional information.

---

[55] Facebook Government requests reports, available via https://transparency.facebook.com/

[56] Verizon Transparency Reports, available via http://transparency.verizon.com/

User data requests to Verizon				
Period	Number (#)		Customer selectors (#)	
	Subscriber information	Transactional information	Subscriber information	Transactional information
2013	No data available		473	
1st half of 2014	No data available		362	0
2nd half of 2014	173	0	193	0
1st half of 2015	144	4	165	4
2nd half of 2015	123	0	193	0
1st half of 2016	168	0	233	0
2nd half of 2016	88	1	132	1
1st half of 2017	116	0	213	0
2nd half of 2017	133	0	229	0
1st half of 2018	153	0	575	0

II. Principles of Telecommunications Interception in Constitutional and Criminal Procedure

A. Constitutional Safeguards of Telecommunications

1. Areas of constitutional protection[57]

Private communications are protected by the constitutional right to the inviolability of the home (Article 15 of the Constitution), the right to privacy (Article 22 of the Constitution),[58] and the right of secrecy of communications (Article 29 of the Constitution).[59]

---

[57] The Belgian Constitution does not contain an explicit right to the confidentiality and integrity of information systems, nor an explicit right to informational self-determination.

[58] An English version of the Belgian Constitution (version of July 2018, updated following the constitutional revision of 24 October 2017 (Belgian Official Journal of 29 November 2017) is available at https://www.dekamer.be/kvvcr/pdf_sections/publications/constitution/GrondwetUK.pdf

[59] See Paul De Hert and Serge Gutwirth, *Anthologie privacy/Anthologie de la vie privée* (Anthology of privacy), Academic and Scientific Publishers, 2013, p. 28, available at http://www.anthologieprivacy.be/sites/anthology/files/documents/anthologie-privacy-asp_0.pdf

Article 15 of the Constitution reads as follows:

> One's home is inviolable; no house search may take place except in the cases provided for by the law and in the form prescribed by the law.

Article 22 of the Constitution reads as follows:

> Everyone has the right to the respect of his private and family life, except in the cases and conditions determined by the law.
>
> The laws, decrees, and rulings alluded to in Article 134 [competence of the Regions in Belgium] guarantee the protection of this right.

Article 29 of the Constitution reads as follows:

> The confidentiality of letters is inviolable.
>
> The law determines which nominated representatives can violate the confidentiality of letters entrusted to the postal service.

2. Proportionality of access to data

a) Belgian Constitution

The Belgian Constitution does not contain a constitutional principle of proportionality and necessity.

b) Data Protection Act of 30 July 2018

The Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data[60] replaces the Data Protection Act of 8 December 1992. The Act of 30 July 2018 implements the 2016 EU General Data Protection Regulation.[61]

The Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data includes the duty of observance of the principle of proportionality. Article 28, 3° of the Act of 30 July 2018 provides that personal data must be "adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed." However, as mentioned below (see II.A.2.c.), the act contains certain exemptions, for instance, in case of information gathering for police purposes.

---

http://www.anthologieprivacy.be/sites/anthology/files/documents/anthologie-privacy-asp_0.pdf

[60] Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data, *Belgian Official Journal*, 5 September 2018, entry into force on the day of publication (5 September 2018) with some exceptions for specific provisions (see Article 281 of the Act).

[61] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88.

c) Act of 5 August 1992 on the Police Function

Until 7 April 2014 (the date of entry into force of the Act of 18 March 2014),[62] Article 44/1 §1 of the Act of 5 August 1992 on the Police Function was phrased in general terms, allowing the police to gather information and intelligence on persons and groups that showed a concrete interest for the exercise of police functions. De Hert and Vermeulen observed the general nature of this provision and its silence regarding systematic data collection.[63] The Act of 5 August 1992 on the Police Function only mentioned the principle of proportionality and subsidiarity in relation to coercive police powers, more particularly in Article 37 which provides that any use of violence by the police services should be reasonable and in proportion to the pursued goals.

The Act of 18 March 2014 modified Article 44/1 of the Act of 5 August 1992 on the Police Function, the first paragraph now providing that the police services shall only process information and personal data insofar as sufficient, relevant, and not excessive in view of police purposes. This provision therefore also applies to the powers for interception of electronic communication under (preventive) police law (see section I.A.2.b.): the general provision on crime detection and evidence gathering by the police (Article 8 CCP) and the specific provision on access by the police to publicly accessible places (Article 26 of the Act on the Police Function).

Furthermore, the Act of 18 March 2014 created a new Article 44/11/9, the fourth paragraph of which lays down a duty for the intelligence and security services, the Belgian Financial Intelligence Processing Unit (CTIF-CFI),[64] the Home Affairs Federal Public Service – Immigration Office,[65] and the prosecution and investigation services of the Federal Public Services Finance's General Administration Customs and Excise to transfer to the police services data and information that are processed in the context of their functions and that are sufficient, relevant, and not excessive in view of police functions.

---

[62] Act of 18 March 2014 regarding police information management and modifying the Act of 5 August 1992 on the Police Function, the Data Protection Act of 8 December 1992, and the Code of Criminal Procedure, *Belgian Official Journal*, 28 March 2014, entry into force on 7 April 2014.

[63] Paul De Hert and Mathias Vermeulen, "Toegang tot sociale media en controle door politie. Een eerste juridische verkenning vanuit mensenrechtelijk perspectief" (Access to social media and control by the police: a first legal exploration from the human rights perspective), *Panopticon*, 2012, vol. 33(2), p. (258) 261.

[64] The CTIF-CFI is the Belgian preventive anti-money laundering and counter-terrorist financing system. *De Cel voor Financiële Informatieverwerking* (CFI, in Dutch), *La Cellule de Traitement des Informations Financières* (CTIF, in French).

[65] *Federale Overheidsdienst (FOD) Binnenlandse Zaken – Vreemdelingenzaken* (in Dutch), *Service Public Fédéral (SPF) Intérieur – Office des étrangers* (in French).

d) Investigation methods

Regarding the legal regime of criminal law, the principle of proportionality and necessity is found in relation to most, but not all, of the legal provisions for intercepting electronic communication. The principle is foreseen for all normal investigation methods, except for data seizure (Article 39*bis* CCP) and preservation requests for natural persons or legal persons (Article 39*ter* CCP). Thus, the investigation methods to which the principle applies are the following: non-secret (network) searches (Article 39*bis* CCP), preservation requests for foreign authorities (Article 39*quater* CCP), the collection of identification data of electronic communications (Article 46*bis* CCP), cyber infiltration (Article 46*sexies* CCP), the tracing of traffic data, and localization of electronic communications (Article 88 CCP), the network searches during looking-in operations (Article 89*ter* CCP), and secret interceptions and secret (network) searches (Article 90*ter* CCP).

e) National collective agreement on the protection of the private lives of employees with respect to controls on electronic online communications data

The national collective agreement on the protection of the private lives of employees with respect to controls on electronic online communications data, signed by Belgium's National Labour Council on 26 April 2002,[66] covers all online technologies, such as the Internet, email, and Wireless Application Protocol (WAP), and has been drafted in sufficiently broad terms to also cover future developments. The agreement seeks to clarify and complement Article 8 of the ECHR, Article 22 of the Constitution (constitutional right to privacy), and the Data Protection Act of 8 December 1992.[67] The obligations of the employer must respect the principle of proportionality: the controls impinging on an employee's private life must be kept to a minimum (Article 6); only data that is necessary for the control purpose may be collected or processed, i.e., data that affects the private life of the employee must be collected to the minimum possible degree.

---

[66] National Labour Council, "National collective agreement no. 81 of 26 April 2002 on the protection of the private lives of employees with respect to controls on electronic online communications data," 26 April 2002, available via www.cnt-nar.be. For a discussion of the agreement, see Paul De Hert, "C.A.O. no. 81 en advies no. 10/2000 over controle van Internet en e-mail" [Labour law: Soft law on e-mail and Internet practices], *Rechtskundig weekblad*, 2002-2003, vol. 66/33, 19 April 2003, pp. 1281–1294.

[67] As noted earlier (section II.A.2.b), the Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data replaces the Data Protection Act of 8 December 1992.

3. Consequences for the interception of telecommunications

The effective protection of the secrecy of telecommunications and the core area of privacy is guaranteed in several ways.

First, the right to privacy (Article 22 of the Constitution) applies to several spheres in the law of criminal procedure, including:[68]

– the secrecy of correspondence: Article 28*septies* §1 and Article 57 §1 CCP require the secrecy of correspondence on the part of everyone who contributes to the preliminary investigation and the investigation respectively. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code (CC). The following articles recall the principle of the secrecy of correspondence: Article 39*ter* CCP (the preservation request for natural persons or legal persons), Article 46*bis* CCP (the collection of identification data of electronic communications), Article 39*ter* CCP (preservation-national), Article 88*bis* CCP (tracing of traffic data, and localization of electronic communications), Article 88*quater* CCP (cooperation with individuals and the private sector regarding the network search), and Article 90*quater* CCP;
– the specific provision with higher standards for the secret interception and secret (network) search (Article 90*ter* CCP);
– the respect for professional secrecy: Article 46*quinquies* juncto Article 89*ter* CCP (looking-in operations), Article 88*bis* §3, Article 90*sexies* §3, and Article 90*octies* CCP (see below, section II.A.4.b.).

Second, data collection by police services and law enforcement authorities is subject to the following control mechanisms (see also below on remedies against interception orders, section III.B.10.b.).

– The Act of 18 March 2014[69] inserted a new Article 44/6 into the Act of 5 August 1992 on the Police Function, which foresees the establishment of a monitoring body for police information.[70]
– The Courts in Chambers (a court of instruction in the first instance)[71] and the Indictment Chamber (a court of instruction in appeal)[72] evaluate the legality of

---

[68] Brigitte Pesquié (revised by Yves Cartuyvels), "The Belgian system, " in Mireille Delmas-Marty and John R. Spencer, *European Criminal Procedures*, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2002, p. (81) 89.

[69] Act of 18 March 2014 regarding police information management and modifying the Act of 5 August 1992 on the Police Function, the Data Protection Act of 8 December 1992, and the Code of Criminal Procedure, *Belgian Official Journal*, 28 March 2014, entry into force on 7 April 2014.

[70] *Het Controleorgaan op de politionele informatie* (in Dutch), *L'Organe de contrôle de l'information policière* (in French).

[71] *Raadkamer* (in Dutch), *Chambre du conseil* (in French).

[72] *Kamer van Inbeschuldigingstelling* (in Dutch), *Chambres des mises en accusation* (in French).

the evidence collection during the investigation phase (Articles 131, 135 §2, and 235*bis* §6 CCP).[73]

Third, exclusionary rules demand the exclusion of illegally obtained evidence (see section IV.2.).

Finally, criminal liability exists for the unlawful infringement of telecommunications (see section II.A.4.a.).

4. Statutory protection of personal data

a) Criminal liability for the unlawful infringement of telecommunications[74]

This section only addresses criminal liability for unlawful infringements that necessarily target telecommunications.[75] It therefore does not discuss non-criminal liability for the unlawful infringement of telecommunications.[76]

---

[73] Brigitte Pesquié (revised by Yves Cartuyvels), "The Belgian system," in Mireille Delmas-Marty and John R. Spencer, *European Criminal Procedures*, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2002, (81) 87, 97.

[74] This section is partially based on the authors' earlier work: Paul De Hert and Gertjan Boulet, "Cybercrime report for Belgium," *International Review of Penal Law (RIDP / IRPL)*, 2013, issue 84, no. 1-2, pp. 12–59, and *Electronic Review of the International Association of Penal* Law, 2013, available via http://www.penal.org/en/reaidp-2013-e-riapl-2013; see also Paul De Hert and Frédéric Van Leeuw, "Cybercrime Legislation in Belgium," in Eric Dirix and Yves-Henri Leleu (eds.), *The Belgian reports at the Congress of Washington of the International Academy of Comparative Law*, Brussels, Bruylant, 2011, pp. 867–956, available at http://www.vub.ac.be/LSTS/pub/Dehert/389.pdf

[75] The following unlawful infringements do not necessarily target telecommunications: child pornography (Articles 383 and 383*bis* CC); grooming (Article 380*ter* §2 CC); stalking (Article 442*bis* CC for normal stalking, and Article 145 §3*bis* of the Act of 13 June 2005 on electronic communications for online stalking); defamation (libel, slander) (Article 443 CC); online gambling (see the Act of 10 January 2010 on gambling, *Belgian Official Journal*, 1 February 2010, entry into force on 1 January 2011); infringements of copyright (see the Act of 19 April 2014 inserting a book XI on 'intellectual property' into the Code of Economic Law, *Belgian Official Journal*, 12 June 2014, entry into force on 1 January 2014; the Act repealed the copyright Act of 30 June 1994, *Belgian Official Journal*, 27 July 1994, entry into force on 1 August 1994); the protection of databases and the rights of the producers of the databases (the Act of 19 April 2014 also repealed the Act of 31 August 1998 transposing the European directive from 11 March 1996 on the juridical protection of databases, *Belgian Official Journal*, 14 November 1998, entry into force on 14 November 1998); abuse registration of a domain name (see the Act of 15 December 2013 inserting book XII on " Law of the electronic economy" in the Code of Economic Law, *Belgian Official Journal*, 14 January 2014, entry into force on 31 May 2014. The Act repealed the Act of 26 June 2003 about the abuse of registration of a domain name, *Belgian Official Journal,* 9 September 2003, entry into force on 19 September 2003); provisions criminalizing racism and holocaust denial (see, for instance, the Act of 30 July 1981 to suppress certain acts inspired by racism and xenophobia, *Belgian Official Journal*, 8 August 1981, entry into force on 18 August 1981); and press crimes (judicial interpretation of the right to freedom of expression and freedom of the press as shaped by Articles 19, 25, and 150 of the Constitution).

aa) Traditional offences in the Belgian Criminal Code

Traditional offences in the Belgian Criminal Code are identity theft (Article 231 CC), trespassing (Article 439 CC), violations of professional secrecy (Article 458 CC), and the secrecy of communications (Article 460 CC).

bb) The protection and interception of electronic communications: the Act of 30 June 1994

The Act of 30 June 1994 protecting privacy against the interception of communications and telecommunications[77] regulates both the protection and the interception of electronic communications. The Act introduced Article 314*bis* into the Belgian Criminal Code, which lays down the prohibition, applicable to everyone, of taking cognisance of the contents of electronic communications one does not participate in during the transfer of the electronic communications. A similar prohibition was introduced for public officials in Article 259*bis* CC.

The Act of 25 December 2016 extends the privacy criminal offences in Articles 259*bis* and Article 314*bis* to the "possession" of communications or data from a computer system that has been unlawfully intercepted or recorded or of which unlawful cognizance has been taken.

However, it should be noted that the monitoring measure in Article 90*ter* CCP provides an exception to the theoretical prohibition of the interception of electronic communications.

cc) The Computer Crime Act of 28 November 2000

The Computer Crime Act of 28 November 2000[78] introduced new penal legislation concerning computer crimes in Belgium. The Act introduced new provisions

---

[76] Non-criminal liability for the unlawful infringement of telecommunications follows from infringements of the national collective agreement of 26 April 2002 on the protection of the private lives of employees with respect to controls on electronic on-line communications data (see section II.A.2.). The collective agreement of 26 April 2002 was declared legally binding by Royal Decree of 12 June 2002 declaring legally binding the national collective agreement of 26 April 2002 on the protection of the private lives of employees with respect to controls on electronic online communications data, *Belgian Official Journal*, 29 June 2002, entry into force on 9 July 2002.

Article 189 of the Social Criminal Code of 6 June 2010 (*Belgian Official Journal*, 1 July 2010, entry into force on the same day) provides that infringements of generally legally binding declared collective agreements shall be punished by a level 1 sanction, to be multiplied by the total number of employees involved. Article 101 of the Social Criminal Code provides that a level 1 sanction consists of an administrative fine of 10 to 100 euros.

[77] Act of 30 June 1994 protecting privacy against the interception of communication and telecommunication, *Belgian Official Journal*, 24 January 1995, entry into force on 3 February 1995.

[78] *Wet inzake informaticacriminaliteit* (in Dutch), *Loi sur la criminalité informatique* (in French), *Belgian Official Journal*, 3 February 2001, entry into force on 13 February 2002.

into the Code of Criminal Law and the Code of Criminal Procedure. The law created the crime of computer forgery[79] (Article 210*bis*), computer fraud[80] (Article 504*quater*), hacking (Article 550*bis*), and sabotage of computer data/data and system interference[81] (Article 550*ter*).

dd) The Act of 13 June 2005 on electronic communications

Article 124 §§1, 3 of the Act of 13 June 2005 on electronic communications protects the content of emails. Under Article 124 of the Act, the following actions are regarded as crimes unless the consent of all parties involved has been given:

1. intentionally taking note of information of all kinds[82] that originates from and is addressed to others;
2. intentionally identifying the persons involved in the transmission of the information and its content;
3. intentionally taking note of electronic communications data and data that relates to other persons;
4. modifying, destroying, disclosing or using in any way the information, identification, and data set forth in 1, 2, and 3 above.

The Act of 13 June 2005 on electronic communications also contains a special penal provision in Article 145 §3, 1° that punishes anyone who carries out fraudulent electronic communications through an electronic communications network. The provision can be used to prosecute hacking.

ee) The Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data

The Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data imposes obligations on data controllers both in the public and in the private sector, although certain exemptions do exist, for instance in the case of information gathering for police purposes. The criminal provisions of the Act (Articles 222 to 230) provide a whole range of sanctions for the data controller who, if failing to meet his obligations, would jeopardize the confidentiality of data. These sanctions will undoubtedly apply to certain uses of personal data threatening the identity data of a person. Article 222 of the Act in particular is, in theory at least, a very suitable instrument to combat identity theft, hacking, secret surveil-

---

[79] *Valsheid in informatica* (in Dutch), *faux en informatique* (in French).

[80] *Informaticabedrog* (in Dutch), *fraude informatique* (in French).

[81] *Informaticasabotage* (in Dutch), *sabotage de données informatiques* (in French).

[82] For example, signs, signals, writings, images, sounds, or data of any nature.

lance, and websites with sensitive data hosted by individuals without permission, such as websites about suspected sex offenders.

b) Protection of professional secrets in criminal procedural law

Article 46*quinquies* juncto Article 89*ter* CCP (looking-in operations) provide a special rule for measures targeted at lawyers and doctors: if the private place is a home or the office of a lawyer of doctor, then the investigating judge (instead of the public prosecutor) has to authorize the measure.

The data retention Act of 29 May 2016 added a new paragraph 3 on professional secrecy to Article 88*bis* CCP (tracing of traffic data, and localization of electronic communications). The new paragraph 3 reflects Article 90*octies* CCP (secret interception and secret (network) search)), and reads as follows:

> The measure can only cover the electronic communication means of a lawyer or a doctor, if they are themselves suspected of having committed or participated in a criminal offence referred to in the first paragraph, or if precise facts suggest that third parties suspected of having committed a criminal offence referred to in paragraph 1, use their electronic communication means.
>
> The measure may not be implemented without, depending on the case, the president of the Bar Association or the representative of the provincial council of the Order of Physicians being informed. Those will be informed by the investigating judge of what according to him shall be covered by professional secrecy. These data shall not be recorded in the official record. These persons are bound by secrecy. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code.

Articles 90*sexies* and 90*octies* CCP provide special rules for secret interception and secret (network) search measures targeted at lawyers and doctors.

Article 90*sexies* §3 provides the following:

> The non-publicly accessible communication or data of a computer system covered by professional secrecy shall not be included in the official report. This communication or data is deposited at the Registry in a file under sealed envelope.[83] In the case of persons referred to in Article 90octies, the matter shall be dealt with as provided in that article.

Article 90*octies* CCP reads as follows:

> §1. The measure can only relate to the premises used for professional purposes, the domicile, the communication means or the computer systems of a lawyer or doctor, if they are themselves suspected of have committed or participated in one of the criminal offenses referred to in Article 90ter, or if precise facts suggest that third parties suspected of having committed one of the offenses referred to in Article 90ter use their premises, domicile, communication means or computer systems.

---

[83] The Act of 5 February 2016 added the specification that "[s]uch (tele-)communications shall be kept at the Registry in a sealed envelope." Act of 5 February 2016 regarding the modification of criminal law and criminal procedure and regarding diverse provisions on criminal policy, *Belgian Official Journal*, 19 February 2016, entry into force on 29 February 2016.

§2. The measure may not be executed without informing the president of the Bar Association or the representative of the provincial council of the Order of Physicians, as the case may be.

These persons are bound by secrecy. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code.

§3. The investigating judge, after consultation with the president of the Bar Association or the representative of the provincial council of the Order of Physicians, shall assess which parts of the communication or data of a computer system referred to in article 90sexies, § 3, which he deems relevant for the investigation, are covered by professional secrecy and which are not.

Only the parts of the communication or data referred to in the first paragraph that are deemed not to be covered by professional secrecy will be transcribed or minuted and, if necessary, translated. The investigating judge shall have an official report drawn up. The files containing this communication or data are deposited at the Registry under sealed envelope.

All other communication or data shall be deposited at the Registry in a separate file under separate sealed envelope.

c) Principle of "purpose limitation of personal data"

Article 15, 1° of 5 August 1992 on the Police Function reads as follows:

> In the performance of their judicial police functions, the police services have the task: 1° to detect the crimes, misdemeanours and contraventions, to gather evidence thereof, to notify the competent authorities thereof, to apprehend, the perpetrators, to arrest them, and to bring them at the disposal of the competent authorities, in the manner and forms provided by law;

Furthermore, as mentioned above (section II.A.2.c.), the Act of 18 March 2014 inserted a new Article 44/1 into the Act of 5 August 1992 on the Police Function, which provides that the police services shall only process information and personal data insofar as sufficient, relevant, and not excessive in view of police purposes.

Similarly, data gathering practices of public prosecutors and investigating judges should be seen in light of their functions in conjunction with the prosecution and investigation of criminal offences. Article 28*bis* §1 CCP provides that "[t]he preliminary investigation is the whole of actions aimed at the detection of crimes, their perpetrators and evidence, and to collect the information relevant for the purposes of criminal proceedings." Article 55 CCP provides that "the investigation is the whole of action aimed at the detection of the perpetrators of crimes, to collect evidence and to take measures that allow the courts to pass informed judgments."

The Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data imposes data protection obligations, including the principle of purpose limitation, on data controllers in the public and private sectors. However, as noted earlier (section II.A.2.c.), the Privacy Act contains some exemptions, e.g., for police purposes.

B. Powers in the Code of Criminal Procedure

1. Requirement of (reasonable) clarity for powers in the law of criminal procedure

The *nullum crimen sine lege* principle also applies in the area of criminal procedure.[84] Article 12(2) of the Constitution reads as follows:

> The freedom of the individual is guaranteed.
>
> No one can be prosecuted except in the cases provided for by the law, and in the form prescribed by the law.
>
> Except in the case of flagrante delicto, no one can be arrested except by virtue of a reasoned order from the judge that must be served not later than forty-eight hours of the deprivation of liberty and can only serve as provisional detention.

In his doctoral thesis on police powers and human rights, Goossens (former attorney-at-law, now member of the Standing Police monitoring Committee[85]) adopts the definition of the legality principle in the criminal procedural sense as proposed by Traest:[86] a legal basis, which moreover should specify the competent authorities as well as the conditions under which the exercise of the investigation methods may involve the infringement of human rights protected by the ECHR.[87]

Goossens further embraces Dupont's description of the legality principle as one of the most fundamental principles of criminal law and as a legal protective principle that finds its historic roots in a reaction against government arbitrariness in the criminal justice system of the Ancien Régime.[88]

The principle of strict interpretation of criminal law, and the related prohibition of an analogous application of criminal law, is closely related to the principle of legality.[89] Legal doctrine traditionally discusses the prohibition of analogous application under criminal law rather than under the law of criminal procedure. Before the adoption of the Act of 25 December 2016, which reworded "telecommunica-

---

[84] The principle also applies in the area of preventive police law. Article 1, §3 of the Act of 5 August 1992 on the Police Function provides that the police services shall only use coercive methods under the conditions determined by law.

[85] *Vast Comité van toezicht op de politiediensten* (*Comité P*, in Dutch), *Comité permanent de contrôle des services de police* (in French).

[86] Franky Goossens, *Politiebevoegdheden en mensenrechten in België. Rechtsvergelijkend en internationaal onderzoek* (Police powers and human rights in Belgium. Comparative and international research), doctoral thesis, Leuven, 2006, pp. 28–29, available at https://lirias.kuleuven.be/bitstream/1979/420/2/frankydoctoraat.pdf

[87] Philip Traest, "Rechts(on)zekerheid in materieel en formeel strafrecht en strafrechtelijk legaliteitsbeginsel" (Legal uncertainty in material and formal criminal law, and the principle of legality in criminal law), *Rechtskundig Weekblad*, 1993-1994, pp. (1190) 1192.

[88] Goossens, *op. cit.*, pp. 28, 30; Lieven Dupont, *Beginselen van strafrecht Deel 1* (Principles of criminal law vol. 1), Leuven, Acco, 2004, pp. 28, 29.

[89] Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, p. 80.

tions" in Article 90*ter* CCP (secret interception and secret [network] search) as "electronic communications," Belgian law enforcement authorities already applied Article 90*ter* CCP to electronic communications, thus allowing an analogy between the interception of traditional telecommunications and electronic communications (see below, section III.B.2.).[90] The Act of 25 December 2016 echoes the calls by the annual reports of the Minister of Justice in implementation of Article 90*decies* CCP[91] to modernize the laws regarding wiretapping on the Internet (see below, section III.B.c.).

2. Differentiation and classification of powers in the law of criminal procedure

The preliminary investigation methods in the Belgian law of criminal procedure are based on the distinction between the preliminary investigation/inquiry phase, under the responsibility of the public prosecutor, and the investigation/instruction phase, under the responsibility of the investigating judge who can also use coercive investigation methods.[92] Article 28*bis* §3 CCP provides that:

> [s]ubject to statutory exceptions, the preliminary investigation measures shall not include coercive measures or violate individual rights and freedoms. These measures may, however, include the seizure of goods referred to in Articles 35 and 36ter.

All reactive criminal law powers mentioned under section I.A.2.a. are principally reserved for the investigation phase, except for the data seizure (Article 39*bis* CCP) and the collection of identification data of electronic communications (Article 46*bis* CCP).[93]

III. Powers for Accessing Telecommunications Data in the Law of Criminal Procedure

A. Overview

In this section, we briefly explain the legal provisions for intercepting electronic communications under (reactive) criminal law (see section I.A.2.a.).

---

[90] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, pp. 396, 244 and following.

[91] See above, section I.B.2.a. See, for instance, the 2013 report in implementation of Article 90*decies* CCP, pp. 18, 47, 48.

[92] Brigitte Pesquié (revised by Yves Cartuyvels), "The Belgian system," in Mireille Delmas-Marty and John R. Spencer, *European Criminal Procedures*, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2002, (81) 87.

[93] Without prejudice to the legal notion of mini-instruction, which is the possibility for the public prosecutor, during the preliminary investigation phase, to request the investigating judge to perform any other investigative measures for which only the investigating judge is competent (see above, section I.A.2.b.).

1. Investigation methods

Article 39*bis* CCP (data seizure and non-secret [network] search) provides that the rules on seizure in the CCP apply to the copying, making inaccessible and deletion of data stored in a computer system or a part of it.

Article 39*ter* CCP (preservation request for natural persons or legal persons), inserted by the Act of 25 December 2016, empowers any judicial police officer, where there are grounds to believe that data stored, processed or transferred through a computer system are particularly vulnerable to loss or modification, to order one or more natural persons or legal persons to preserve data in their possession or over which they have control.[94]

Article 39*quater* CCP (preservation request for foreign authorities), inserted by the Act of 25 December 2016, empowers the public prosecutor to request a foreign competent authority to order, or otherwise impose, the expeditious preservation of data that is stored, processed or transferred through a computer system located on the territory of that competent authority and in respect of which a Belgian competent judicial authority intends to submit a request for mutual legal assistance.[95]

Article 46*sexies* CCP (cyber infiltration), inserted by the Act of 25 December 2016, empowers the public prosecutor to authorize police services to maintain contact on the internet, if necessary under a fictitious identity, with one or more persons concerning which there are serious indications that they are committing or would commit criminal offences.

Article 46*bis* CCP (collection of identification data of electronic communications) empowers the public prosecutor to identify 1) the subscriber or the habitual user of an electronic communications service, 2) the electronic communication means used, and 3) the electronic communications services to which a particular person is a subscriber or that are habitually used by a particular person.

Article 88*bis* CCP (tracing of traffic data, and localization of electronic communications) empowers the investigating judge, and in specific cases the public prosecutor, to 1) trace traffic data of electronic communication means from which or to

---

[94] Article 39*ter* CCP embodies the implementation of Articles 16 and 17 of the Cybercrime Convention. Articles 16 and 17 of the Cybercrime resort under Chapter II (measures to be taken at the national level), section II (procedural law) of the Convention. The title of Article 16 of the Cybercrime Convention is "Expedited preservation of stored computer data;" the title of Article 17 of the Cybercrime Convention is "Expedited preservation and partial disclosure of traffic data."

[95] Article 39*quater* CCP embodies the implementation of Articles 29 and 30 of the Cybercrime Convention. Articles 29 and 30 of the Cybercrime resort under chapter III (international co-operation), section 2 (specific provisions) of the Convention. The title of Article 29 of the Cybercrime Convention is "Expedited preservation of stored computer data"; the title of Article 30 of the Cybercrime Convention is "Expedited disclosure of preserved traffic data."

which electronic communications are or were made, 2) locate the origin or the destination of electronic communications.

Article 89*ter* CCP (network search during looking-in operations) empowers the investigating judge, in the context of the execution of the measure provided for in Article 46*quinquies* CCP (looking-in operations), to gain access to a computer system and to search it.

Article 90*ter* CCP (secret interception and secret (network) search) empowers the investigating judge, and in specific cases the public prosecutor, with a secret purpose, to intercept, take cognizance of, search and record non-publicly accessible communication or data from a computer system or part of it with technical means, or extend the search in a computer system or part of it.

3. Cooperation with individuals and the private sector

For the execution of the above-mentioned investigation operations, Belgian law enforcement agencies can cooperate with individuals and the private sector (Article 39*bis*, Article 46*bis*, Article 88*bis*, Article 88*quater*, Article 90*quater* §§2, 4 CCP).

Article 39*bis* CCP (data seizure) allows the public prosecutor to request an Internet Service Provider (ISP) to delete the domain name of a site that violates the law from their Domain Name Server (DNS).

Article 39*bis* §5 CCP authorizes the public prosecutor or the investigating judge to order the temporary suspension of security or the application of technical means to decipher and decode the data.[96]

Article 39*ter* CCP (preservation request for natural persons or legal persons) empowers any judicial police officer, where there are grounds to believe that data stored, processed or transferred through a computer system is particularly vulnerable to loss or modification, to order one or more natural persons or legal persons to preserve data in their possession or over which they have control.

Article 46*bis* CCP (collection of identification data of electronic communications) obliges operators of an electronic communications network and providers of an electronic communications service to provide identification data upon request of the public prosecutor.

Article 88*bis* CCP (tracing of traffic data, and localization of electronic communications) obliges operators of an electronic communications network and provid-

---

[96] The investigating judge has exclusive authority to order these measures when this is particularly necessary to extend the search in a computer system (or part of it) to a computer system (or a part of) in a different location.

ers of an electronic communications service to provide traffic or localization data upon request of the public prosecutor.

Article 88*quater* CCP (cooperation with individuals and the private sector regarding the network search) allows the public prosecutor to impose on certain individuals the obligation to cooperate during an investigation. These individuals are persons of whom the investigating judge thinks that they have special capacities/knowledge of the computer system that is the object of an investigation or of services used to store, process, encrypt, or transfer data.

Article 90*ter* CCP reflects Article 39*bis* §5 CCP (data seizure) regarding the authorization of the investigating judge to order the temporary suspension of security or the application of technical means to decipher and decode the data.

Article 90*quater* §2 CCP (secret interception and secret [network] search) obliges operators of an electronic communications network and providers of an electronic communications service to provide cooperation with a secret interception and secret (network) search under Article 90*ter* CCP.

Article 90*quater* §4 (secret interception and secret [network] search) echoes the cooperation referred to in Article 88*quater* CCP, i.e., the power (for the investigating judge, not the public prosecutor) to impose an obligation to cooperate on individuals which the investigating judge considers to have special capacities/knowledge of the computer system that is the object of an investigation or of services used to store, process, encrypt, or transfer data.

Belgian law enforcement agencies can also cooperate with providers of private electronic communications networks and electronic communications services that are not publicly available (so-called closed groups of end-users)[97] on the basis of Articles 122, 125, and 127 of the Electronic Communications Act[98] and with service providers acting as a mere conduit, catching and hosting on the basis of Articles XII.17 till XII.20 of the Code of Economic Law.[99]

Furthermore, in specific cases, judicial authorities can order a temporary surveillance period for Internet service providers acting as a mere conduit, catching and hosting (Article XII.20 of the Code of Economic Law).

---

[97] For example, access to corporate networks is limited to members of the corporation.

[98] Article 9 §7 of the Electronic Communications Act of 13 June 2005 (*Belgian Official Journal*, 20 June 2005, entry into force on 30 June 2005) provides that a specific Royal Decree shall address the matter of the cooperation between law enforcement agencies and providers of private electronic communications networks and electronic communications services that are not publicly available (closed user groups), under the conditions determined by Articles 46*bis*, 88*bis* and 90*ter* to 90*decies* of the CCP.

[99] Code of Economic Law of 28 February 2013, *Belgian Official Journal*, 29 March 2013, entry into force on 12 December 2013.

According to legal experts, the big four tech companies (GAFA)[100] are reluctant to establish themselves in Belgium considering cooperation duties. They also observed that in cases of serious crime, such as terrorism or child kidnapping, the GAFA rapidly cooperate (including transferring email content).

They also mentioned that Internet of Things (IoT)-providers are obliged to cooperate, such as vehicle companies regarding requests for GPS-data.

4. Data retention

See section I.A.2.dd.

B. Interception of Content Data

1. Statutory provision

Article 90*ter* CCP is the main provision in the law of criminal procedure dealing with the interception of the content of communications. Article 90*ter*, §1 CCP provides the core meaning of the secret interception and secret (network) search:

> […] the investigating judge can, with a secret purpose, intercept, take cognizance of, search and record non-publicly accessible communication or data from a computer system or part of it with technical means, or extend the search in a computer system or part of it.
>
> This measure can only be ordered in exceptional cases, when the investigation so requires, if there are serious indications that it concerns an offence referred to in paragraph 2, and if the other investigation means are not sufficient to reveal the truth.
>
> In order to make this measure possible, the investigating judge can order, at any time, without the knowledge or permission of either the occupant, the owner or his beneficiary, or the user:
>
> – to enter a home, a private place or a computer system;
>
> – to temporarily suspend all security of the computer systems concerned, if necessary with the aid of technical means, false signals, false keys or false capacities;
>
> – to install technical means in the computer systems concerned, in order to decipher and decode the data stored, processed or forwarded by that system.
>
> The measure referred to in this section can only be ordered to trace the data that can serve to reveal the truth. The measure can only be ordered in respect of persons suspected of having committed the criminal offence on the basis of precise facts, in respect of communication means or computer systems frequently used by a suspected person or in respect of the places where he is suspected to stay. The measure can also be ordered in respect of persons who are suspected on the basis of precise facts to be in regular contact with a suspected person.

---

[100] Google, Apple, Facebook, and Amazon.

2. Scope of application

a) Object of interception

As noted (see section II.B.1.), before the adoption of the Act of 25 December 2016, which reworded "telecommunications" in Article 90*ter* CCP as "electronic communications," Belgian law enforcement authorities already applied Article 90*ter* CCP to electronic communications, thus allowing an analogy between the interception of traditional telecommunications and electronic communications.

The parliamentary preparatory works provide that the term (tele-)communications has a broad scope, including any linguistic expression, verbal or non-verbal, whether directly or from a physical distance, and irrespective of the number of participants. The term includes monologues, telegrams, telex, telefax, and electronic data transfers in computers and computer networks.[101]

The annual reports of the Minister of Justice in implementation of Article 90*decies* CCP provide data for the following objects of the wiretapping measure: landline numbers, mobile numbers, IMEI numbers, and email (see section I.B.2.).

Kerkhofs and Van Linthout further specify that Article 90*ter* CCP covers the following forms of communication:[102]

- classical telecommunications: analogous communication (voice and data) via landlines (landline numbers), and mobile communications;
- pop-mail: e.g., Microsoft Outlook, Mozilla Thunderbird, Apple Mail;
- webmail: e.g., Yahoo, Gmail, MSN, Hotmail;
- voiceover IP (VoIP): e.g., Viber, Skype;
- instant Messaging (IM) via
  - private chatrooms: e.g., Paltalk.com;
  - online gaming applications: e.g., World of Warcraft;
  - virtual gaming worlds: e.g., Second Lige;
  - mobile applications: e.g., WhatsApp, Google Talk, Blackberry Messenger.

IP data does not constitute private communications and therefore does not fall under the scope of Article 90*ter* CCP.

---

[101] Parliamentary preparatory works, Belgian Senate, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, 1992–1993, 1 September 1993, 843-1, p. 7, available at http://www.senate.be/lexdocs/S0539/S05390297.pdf; Parliamentary preparatory works, Belgian Senate, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, 1993–1994, 18 May 1994, 843-2, p. 38, available at http://www.senate.be/lexdocs/S0539/S05390364.pdf

[102] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, pp. 279, 282, 295.

The available annual reports of the Minister of Justice as regards the implementation of Article 90*decies* CCP (until 2013) do not show cases of wiretapping clouds or communications between two independent computer systems (e.g., between an automated machine and its computer-based automated control center, especially in the "Internet of things"). But as noted, legal experts mentioned the possibility to request cooperation from IoT-providers (see section I.A.2.cc.).

b) Temporal limits of telecommunications

aa) Access to ongoing telecommunications

Before the Act of 25 December 2016, the wiretapping measure (Article 90*ter* CCP) only applied to (tele-)communications "during transmission."[103] The network search in former Article 88*ter* CCP was applied to intercept "stored data." The Act of 25 December 2016 embodies the secret network in Article 90*ter* CCP, which nullifies the former legal distinction between interception of "data in transmission" (subject to Article 90*ter* CCP) and interception of "stored data" (subject to former Article 88*ter* CCP).[104]

bb) Access after the end of telecommunications transmission

As said (section III.B.2.b.aa.), Article 90*ter* CCP also applies to stored data after the transmission process.

---

[103] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 288.

[104] For Kerkhofs and Van Linthout, the transmission phase ended at the so-called "indicated terminal," i.e., the place where an email was deemed to arrive considering its nature and the user email configuration. They specified that, whereas the indicated terminal of "pop-mail" is principally the user's own computer, the indicated terminal of "webmail" is principally the user's online webmail account. Hence, pop-mail that arrives in an online web mailbox was still deemed to be in transmission, whereas webmail that arrives in an online web mailbox was deemed to be out of transmission and therefore beyond the scope of the monitoring measure of Article 90*ter* CCP. In the latter case, law enforcement authorities used a network search (former Article 88*ter* CCP) to access the data. In practice, however, pop-mail may de facto be configured as webmail, and vice versa. In case of doubt, law enforcement authorities issued a combined warrant: "90*ter* CCP versus 88*ter* CCP" (or vice versa).

Kerkhofs and van Linthout also observed that a wiretapping measure was possible in case of misuse of webmail, such as the sharing of one webmail account between different users in order to exchange messages via emails stored in the draft folder. In this case, the transmission phase ends after the recipient of the draft email reads the draft email by the recipient. Thus, in this case the end of the transmission phase is conditioned by the "reading" of emails, instead of the arrival on the user's own computer or online webmailbox.

c) Current matters of dispute

By nullifying the former legal distinction between the interception of "data in transmission" (subject to Article 90*ter* CCP) and the interception of "stored data" (subject to former Article 88*ter* CCP), the Act of 25 December 2016 seems to have solved dispute matters regarding the determination of the transmission phase.

However, constitutional reasoning regarding the scope of privacy and criminal law protection, such as the protection against the interception of (tele-)communications offered by Article 314*bis* and Article 259*bis* CC, could affect discussions regarding the scope of the interception measure.

For example, as noted (section III.B.2.b.aa.), before the Act of 25 December 2016, Kerkhofs and Van Linthout wrote that pop-mail arriving in an online web mailbox is still deemed to be in transmission and therefore can be intercepted on the basis of Article 90*ter* CCP. Dewandeleer confirmed this view, which is based on a judgment of 4 December 2007 of the Correctional Court of Leuven.[105]

Arnou, on the other hand, argued against wiretapping any email (both pop-mail and webmail) stored on the server.[106] In other words, the transmission phase for an email would always end at the moment of its arrival in the online webmailbox. His reasoning echoes the parliamentary preparatory works of 1998 modifying the Act of 30 June 1994 protecting privacy against the interception of communication and telecommunication, which state that emails stored on the server of a service provider do not enjoy the privacy protection against the interception of (tele-)communications (Article 314*bis* and Article 259*bis* CC, see section II.A.4.) but are possibly protected by other criminal laws. Therefore, the parliamentary preparatory works provide that such emails cannot (more precisely: do not have to) be intercepted on the basis of Article 90*ter* CC but on the basis of other investigation methods, such as the powers of search and seizure (Article 39*bis* CCP) and the network search (former Article 88*ter* CCP).[107]

---

[105] Dirk Dewandeleer, "De kennisname van e-mails 'tijdens de overbrenging ervan', een verduidelijking van het telecommunicatiegeheim" (Taking knowledge of e-mails during the transmission phase. A clarification of the secrecy of telecommunications), annotation to the judgment of the Correctional Court of Leuven, 4 December 2007), *Tijdschrift voor Strafrecht*, 2008, vol. 3, p. [226] 226.

[106] Luc Arnou, "Afluisteren tijdens het gerechtelijk onderzoek" (Wiretapping during the investigation); in Commentaar Strafrecht en strafvordering (Commentary criminal law and criminal procedural law), Gent, Kluwer, 2008, vol. 59, pp. 13–14, no. 12.

[107] Parliamentary preparatory works, Belgian Chamber of Parliaments, modifying the Act of 30 June 1994 protecting privacy against the interception of communication and telecommunication, 1996-1997, 29 May 1998, no. 49K1075/017, p. 10, available at http://www.dekamer.be/FLWB/PDF/49/1075/49K1075017.pdf

3. Special protection of confidential communications content

a) Privileged communications

aa) Professional secrets

(1) Conditional protection of lawyer's and doctor's secrets against the interception measure: only after notification to the Bar Association or the representative of the provincial council of the Order of Physicians

Article 90*octies* §§1–2 read as follows:

> §1. The [interception] measure can only relate to the premises used for professional purposes, the domicile, the communication means or the computer systems of a lawyer or doctor, if they are themselves suspected of have committed or participated in one of the criminal offenses referred to in Article 90ter, or if precise facts suggest that third parties suspected of having committed one of the offenses referred to in Article 90ter use their premises, domicile, communication means or computer systems.
>
> §2. The measure may not be executed without informing the president of the Bar Association or the representative of the provincial council of the Order of Physicians, as the case may be.
>
> These persons are bound by secrecy. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code.

A contrario, notification to the president of the Bar Association or the representative of the provincial council of the Order of Physicians may not be necessary for an interception measure concerning targets other than "the premises used for business purposes, the domicile, the communication means or the computer systems of a lawyer or a doctor."

Arnou and Freyne consier that the notification duty is satisfied in case of a written notification or confirmation of an oral notification in an official record.[108] Although notification to the president of the Bar Association or the representative of the provincial council of the Order of Physicians is not prescribed under sanction of nullity (see below on exclusionary rules, section IV.2.), the parliamentary preparatory works underline that the public order nature of this provision implies that failure to do so will entail the nullity of the interception measure.[109] As noted below

---

[108] Luc Arnou, "Afluisteren tijdens het gerechtelijk onderzoek" (Wiretapping during the investigation); in Commentaar Strafrecht en strafvordering (Commentary criminal law and criminal procedural law), Gent, Kluwer, 2008, vol. 59, p. 36, no. 33; Thierry Freyne, "De bewaking van privécommunicatie en telecommunicatie in strafonderzoeken: een stand van zaken" (The monitoring of private communications and telecommunications in criminal proceedings: a state of affairs), *Tijdschrift voor Strafrecht*, 2008, vol. 3, p. 177, no. 33.

[109] Parliamentary preparatory works, Belgian Senate, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, 1993–1994, 18 May 1994, no. 843-2, p. 189, available at http://www.senate.be/lexdocs/S0539/S05390364.pdf

(section IV.4.c), in a judgment of 18 February 2003,[110] the Supreme Court held that the rights of the defence may justify access by the defence to the documents resulting from a nullified investigation method. In fact, these documents are not deleted but kept at the Registry in a sealed envelope (Article 235*bis* §6 CCP).

(2) Unconditional protection of professional secrets against inclusion in official records

Article 90*sexies* §3 CCP protects all possible professional secrets, such as communication between an attorney-at-law and a client, a medical practitioner and a patient, journalists' communications, communication under the law regulating financial and banking secrecy, etc. The provision provides that "[t]he non-publicly accessible communication or data of a computer system covered by professional secrecy shall not be included in the official report. This communication or data is deposited at the Registry in a file under sealed envelope. In the case of persons referred to in Article 90octies [docters and lawyers], the matter shall be dealt with as provided in that article."

Article 90*sexies* §3 *in fine* CCP, read in conjunction with Article 90*octies* §3, first indent, CCP, provides additional protection for lawyers and doctors:

> Article 90*sexies* §3 *in fine* CCP: In the case of persons referred to in Article 90*octies* [docters and lawyers], the matter shall be dealt with as provided in that article.
>
> Article 90*octies* §3, first indent CCP: The investigating judge, after consultation with the president of the Bar Association or the representative of the provincial council of the Order of Physicians, shall assess which parts of the communication or data of a computer system referred to in article 90*sexies*, § 3, which he deems relevant for the investigation, are covered by professional secrecy and which are not.

The recordings protected by professional secrecy are not recorded in the official record, but kept at the Registry in file under sealed envelope on the basis of Articles 90*septies* §3 and 90*octies* §3 *in fine* CCP.[111]

Article 90*septies* §6 CCP lays down the right for some parties to access a copy of the recorded non-public communication or data from a computer system, of which certain parts that are deemed relevant for the investigation have been transcribed or minuted and included in an official report that they have access to, and also provides cases in which the investigating judge or the court *may* upon request allow access to the recordings deposited at the Registry:

> § 6. The indicted, the accused, the civil party or their lawyers shall receive, on simple request, a copy of the whole of the recorded non-public communication or data from a computer system, of which certain parts that are deemed relevant for the investigation

---

[110] Supreme Court, 18 February 2003, P.02.0913.N.

[111] Thierry Freyne, "De bewaking van privécommunicatie en -telecommunicatie in strafonderzoeken: een stand van zaken" (The monitoring of private communications and telecommunications in criminal proceedings: a state of affairs), *Tijdschrift voor Strafrecht,* 2008, vol. 3, p. 177, no. 30.

have been transcribed or minuted and included in an official report that they have access to.

The indicted, the accused, the civil party or their lawyers may request the judge to consult the other files or documents deposited at the Registry in accordance with § 4, and to transcribe or minute additional parts of the recorded communication or data. The request addressed to the investigating judge shall be dealt with in accordance with Article 61quinquies.

The judge may reject the request if it does not consider the consultation or transcription or minutes of additional parts necessary to reveal the truth, if it considers it detrimental to the investigation at that time, or for reasons related to the protection of other rights or interests of persons. He can also limit the consultation or transcription or minutes of additional parts to a selection of files or documents he has specified.

bb) Protection of the core area of privacy

Article 90*ter* CCP provides no additional protection for the core area of privacy.

b) Responsibility for ensuring protection

The articles discussed in the previous section show that the responsibility for ensuring the protection of professional secrets lies with the investigating judge, thus the magistrate that issues the warrant.

The investigating judge, however, does not have complete discretion to determine the stage of the interception phase in which, and the way in which, these privileges have to be conducted. It is recalled, first, that, according to Article 90*octies* §2, first indent CCP, an interception measure in relation to the premises used for business purposes, the domicile, or the communication means or the computer systems of a lawyer or a doctor may only be implemented *after* notification, depending on the case, to the president of the Bar Association or the representative of the provincial council of the Order of Physicians. Second, according to Article 90*octies* §3, first indent CCP, the investigating judge shall consult with the president of the Bar Association or the representative of the provincial council of the Order of Physicians on which parts of the communication or data of a computer system which he deems relevant for the investigation are covered by professional secrecy, and thus not be recorded in the official record under Article 90*sexies* §3.

However, the president of the Bar Association or the representative of the provincial council of the Order of Physicians does not have have any right of co-decision or contradiction.

4. Execution of telecommunications interception

a) Execution by the authorities with or without the help of third parties

For the execution of an interception measure, law enforcement authorities can use their own technical equipment (see section III.B.4.b.), or cooperate with third parties (see also section III.B.5.a.). Article 90*ter* §1, third indent CCP and Article 90*quater* §§2, 4 CCP lay down the cooperation duties for individuals and the private sector.

Article 90*ter* CCP reflects Article 39*bis* §5 CCP (data seizure) regarding the authorization of the investigating judge to order the temporary suspension of security or the application of technical means to decipher and decode the data. But contrary to Article 39*bis* CCP, Article 90*ter* CCP allows the order without the knowledge of either the owner, the occupant, the owner or his beneficiary, or the user.

Article 90*quater* §2, first indent CCP reads as follows:

> §2. The investigating judge can, in order to make the measure referred to in Article 90ter, §1, possible, directly or through the police service designated by the King,[112] request the cooperation of:
>
> – the operator of an electronic communications network, and
>
> – anyone who, within the Belgian territory, makes available or offers, in whatever way, a service consisting of the transmission of signals via electronic communications networks, or that enables users to obtain, receive or distribute information via an electronic communications network. This also includes the provider of an electronic communications service.[113]

Article 90*quater* §4, first indent CCP reads as follows:

> The investigating judge can order persons of whom he thinks that they have special knowledge of the communication means or the computer system service to which the measure relates, or of services or applications to secure, encode or encrypt data that are stored, processed, or transferred via a computer system, to provide information about its operation and about the way to gain access in an understandable form to its content that is being or has been transferred.

---

[112] The Act of 5 February 2016 amended Article 90*quater* §2, 1° CCP and Article 90*quater* §4, 1-2° CCP, and added the possibility for the investigating judge to request technical cooperation via a police service appointed by the King. Act of 5 February 2016 regarding the modification of criminal law and criminal procedure and regarding diverse provisions on criminal policy, *Belgian Official Journal*, 19 February 2016, entry into force on 29 February 2016.

[113] See also on Article 46*bis* CCP (identification data), Article 88*bis* CCP (traffic and localization data) and Article 464/1 CCP (criminal enforcement investigation): This definition corresponds to the autonomous (broad) interpretation by the Belgian Supreme Court of the term "electronic communications provider" in Article 46*bis* CCP (judgment of 18 January 2011 P.10.1347.N, available via http://jure.juridat.just.fgov.be/).

Media reports have alleged direct access by Belgian law enforcement agencies to the servers of operators and service providers.[114] Vodafone's online presentation of its 2014 law enforcement disclosure report confirms this practice but does not specify which countries allow such direct access:

> However, in a small number of countries the law dictates that specific agencies and authorities must have direct access to an operator's network, bypassing any form of operational control over lawful interception on the part of the operator. In those countries, Vodafone will not receive any form of demand for lawful interception access as the relevant agencies and authorities already have permanent access to customer communications via their own direct link.[115]

In this context, it should be kept in mind that the modalities of the cooperation duties under Article 90*quater* §2 and §4 CCP are laid down in the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications (hereinafter "Royal Decree of 9 January 2003").[116] The Royal Decree installs a Coordination Cell Justice responsible for handling the information requests by Belgian legal authorities. According to Article 4 of the Royal Decree, the Coordination Cell Justice shall transfer the data in real time after receipt of the warrant in Article 90*ter* §1 or §5 CCP. It could therefore be asked whether direct access by law enforcement to the servers of operators and service providers would be compatible with the requirement of a Coordination Cell Justice for law enforcement cooperation.

Also relevant in this regard is the standard TS 101-331 set by the European Telecommunications Standards Institute (ETSI), which is applicable to data transfers in Belgium on the basis of Article 6 §3 of the Royal Decree of 9 January 2003:[117]

---

[114] Cf. The Washington Post, "Do France and Belgium have direct wiretap access to telecom switches?," 7 June 2014, available at http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/07/do-france-and-belgium-have-direct-wiretap-access-to-telecom-switches/

[115] Vodafone, "Law Enforcement Disclosure Report," via https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

[116] Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications, *Belgian Official Journal*, 10 February 2003, entry into force on 10 May 2003; The Royal Decree of 9 January 2003 was amended by the Royal Decree of 8 February 2011 modifying Royal Decree of 9 January 2003 regarding the execution of the Royal Decree of 9 January 2003 regarding the execution of Article 46*bis* §2, paragraph 1, 88*bis* §2, paragraphs 1 and 3 and 90*quater* §2 paragraph 3 CCP and of Article 109*ter* E §2 of the Act of 21 March 1991 on the reform of certain economic public enterprises, *Belgian Official Journal*, 23 February 2011, entry into force on 5 March 2011.

[117] European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.7.g, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

> [T]he result of interception shall only be transmitted to the Law Enforcement Monitoring Facility [LEMF] as indicated in the lawful authorization when proof of the authority to receive of the LEMF, and proof of the authority to send of the interface, has been furnished.

b) Accompanying powers for the execution of interception

Article 90*ter* §1 CCP allows the execution of the interception measure with technical means but does not define this term. Neither does it clarify whether technical means under Article 90*ter* CCP also include technical means that can be used for a looking-in operation, observation and cyber infiltration (see below, section III.D.1.). Furthermore, the parliamentary preparatory works intentionally do not define technical means under Article 259*bis* CC (protection of telecommunications) because of the risk that any definition becomes obsolete due to technological developments.[118] However, the parliamentary preparatory works prohibit the intrusion into a computer system (hacking) for the interception measure of Article 90*ter* CCP.[119]

De Valkeneer notes that technical means under Article 90*ter* CCP include micro-spies, key-loggers, and parabolic microphones outside a home or private place.[120] De Wolf wonders if viruses qualify as technical means under Article 90*ter* CCP.[121]

Belgian law enforcement authorities do not possess a satellite for the interception of electronic communication. Hence, if the investigation so requires, Belgium has to launch a request for mutual legal assistance to a state that has such technical means.[122]

Article 90*ter* §1, third indent CCP also allows the investigating judge, in order to make the interception measure possible, to order, without the knowledge or permission of either the occupant, the owner or his beneficiary, or the user, to enter a home, a private place or a computer system.

---

[118] Parliamentary preparatory works, Belgian Senate, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, 1992-1993, 1 September 1993, no. 843-1, p. 6, available at http://www.senate.be/lexdocs/S0539/S05390297.pdf

[119] Parliamentary preparatory works, Belgian Senate, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, 1992-1993, 1 September 1993, no. 843-1, p. 11, available at http://www.senate.be/lexdocs/S0539/S05390297.pdf

[120] Christian De Valkeneer, *Manuel de l'enquête pénale* (Manual on criminal investigation), Brussels, Larcier, 2006, p. 334.

[121] Daniel De Wolf, "Rapport Belge" (Belgian report on criminal procedure), *Electronic Review of the International Association of Penal Law*, 2014, p. 23, available at http://www.penal.org/sites/default/files/files/RA %20- %203.pdf

[122] See also below (section V.B.3.): Article 90*ter* §§6–7 CCP addresses the interception of electronic communication by another State in cases where the suspect either is situated in border areas where the networks of Belgian and foreign operators intertwine or uses satellite communication.

5. Duties of telecommunications service providers to cooperate

a) Possible addressees of duties of cooperation

As said (section III.B.5.a.), the possible addressees of duties of cooperation are:

– the operator of an electronic communications network (Article 90*quater* §2 CCP);
– anyone who, within the Belgian territory, makes available or offers, in whatever way, a service consisting of the transmission of signals via electronic communications networks, or that enables users to obtain, receive or distribute information via an electronic communications network. This also includes the provider of an electronic communications service (Article 90*quater* §2 CCP);
– persons of whom the investigating judge thinks that they have special knowledge of the communication means or the computer system service to which the measure relates, or of services or applications to secure, encode or encrypt data that are stored, processed (Article 90*quater* §4, first indent CCP).

Hence, the personal scope of application of the cooperation duty is quite broad and includes infrastructure providers working at the IP-transport level (operators of a telecommunications network), Internet Access Providers (IAPs) and Internet Service Providers (ISPs), such as social media providers and cloud computing service providers.

On 23 February 2018, the Court of Appeal of Brussels lodged a request for preliminary ruling by the Court of Justice of the EU, inquiring whether Skype can be considered as an electronic communications provider under Directive 2002/21/EC of 7 March 2002.[123] The answer by the CJEU may have spillover effects in another (still pending) case involving Skype, in which a Belgian investigating judge requested the Luxembourg-based entity Skype to provide technical cooperation in setting up a wiretap on a Skype user. Skype refused to do so on jurisdiction grounds, arguing that Belgian authorities should use the MLA process. Furthermore, Skype claimed technical incapability to set up a wiretap on a Skype user. However, the Court of first Instance and the Court of Appeal judged in favour of the prosecution and fined Skype.[124] The Court of first Instance relied on what the

---

[123] Request for a preliminary ruling from the Cour d'appel de Bruxelles (Belgium) lodged on 23 February 2018 – Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (IBPT), Case C-142/18, available via http://curia.europa.eu

[124] Correctional Court of Mechelen, Public Prosecutor against Skype Comunications SARL, judgment of 27 October 2016, available (in Dutch) via http://www.wolterskluwer.be/files/communities/legalworld/rechtspraak/2016/Corr. %20Mechelen %2027 %20oktober %202016 %20(Skype).pdf ; Court of Appeal of Antwerp, judgment of 15 November 2017, available via https://legalworld.wolterskluwer.be/media/5528/antwerpen-skype.pdf

Supreme Court (in her first judgment in the Yahoo! Case, see section III.C.b.dd.) held, i.e., that the definition of "electronic communications provider" in Article 46*bis* CCP is independent of the definition stipulated in the Act 13 June 2005 on electronic communications. The case is currently pending before the Supreme Court.[125]

b) Content of duties to cooperate

Article 90*quater* §2 CCP pertains to technical cooperation in order to make the measure referred to in Article 90*ter* CCP possible.

Article 90*quater* §4 CCP pertains to the provision of information

– about the operation of the communication means or the computer system service to which the measure relates, or of services or applications to secure, encode or encrypt data that are stored, processed, or transferred via a computer system;
– and about the way to gain access in an understandable form to its content that is being or has been transferred.

The modalities of the cooperation duties under Article 90*quater* §§2, 4 CCP are laid down in the Royal Decree of 9 January 2003. The Royal Decree installs a Coordination Cell Justice responsible for handling the information requests from Belgian legal authorities.

c) Duties to provide technical and organizational infrastructure

aa) Obligated parties

Article 1, 5° of the Royal Decree of 9 January 2003 defines its personal scope of application in terms of the "Internet sector," i.e., the entirety of operators of electronic communications networks and providers of electronic communications services.

bb) Individual technical obligations

Article 6 §3 of the Royal Decree of 9 January 2003 demands that technical standards for data transfers comply with the following updated ETSI standards and reports:

1) TS 101-331: Lawful Interception (LI); Requirements of Law Enforcement Agencies (hereinafter "ETSI TS 101-331");

---

[125] For more information about the discussion regarding Skype's status as a telecom operator, see Mike Conradi, "Lawful intercept on VoIP services – Skype in Belgium," DLA Piper Telecoms blog, 12 March 2018, available via https://www.technologyslegaledge.com/2018/03/lawful-intercept-on-voip-services-skype-in-belgium/

2) TS 101-671: Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic;
3) TS 101-909-20-1: AT Digital. Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services;
4) TS 101-909-20-2 AT Digital. Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services;
5) TR 101-943: Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture;
6) TR 101-944: Lawful Interception (LI); Issues on IP Interception;
7) TR 102-053: Lawful Interception (LI); Notes on ISDN LI functionality;
8) TS 102-232: Lawful Interception (LI); Handover Specification for IP Delivery;
9) TS 102-233: Service-specific details for e-mail services;
10) TS 102-234: Lawful Interception (LI); Service-specific details for internet access services;
11) TS 102-815: Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception;
12) TS 133-10: Universal Mobile Telecommunication System (UMTS); "Lawful interception requirements (3GPP TS 33.106 version 5.1.0 Release 5) [3GPP SA3];
13) TS 133-107: Universal Mobile Telecommunication System (UMTS); 3G security; Lawful interception architecture and functions (3GPP TS 33.107 version 5.5.0 Release 5) [3GPP SA3];
14) TS 133-108: Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful interception (LI) (3GPP TS 33.108 version 5.4.0 Release 5) [3GPP SA3];
15) ES 201-158: Lawful Interception (LI); Requirements for Network Functions;
16) ES 201-671: Lawful Interception (LI): Handover Interface for the Lawful Interception of Telecommunications traffic;
17) Digital cellular telecommunications system (Phase 2+); Lawful interception requirements for GSM (GSM 01.33 version 8.0.0 Release 1999) [TC SMG] TR 101 514;
18) Digital cellular telecommunications system (Phase 2+); Lawful interception – Stage 1 (GSM 02.33 version 8.0.1 Release 1999) [TC SMG] TR 101 507;
19) Digital cellular telecommunications system (Phase 2+); Lawful interception – Stage 1 (3GPP TS 43.033 version 5.0.0 Release 5) [3GPP SA3] TR 143 033;

20) Digital cellular telecommunications system (Phase 2+); Lawful interception – Stage 1 (3GPP TS 42.033 version 5.0.0 Release 5) [3GPP SA3] TR 142 033;
21) Digital cellular telecommunications system (Phase 2+); Lawful interception requirements for GSM (3GPP TR 41.033 version 5.0.0 Release 5) [3GPP SA3] TR 141 033;
22) Digital cellular telecommunications system (Phase 2+) (GSM); Lawful interception – Stage 2 (3GPP TS 03.33 version 8.1.0 Release 1999) [3GPP SA3] TS 101 509.

cc) Organizational obligations

Article 2 of the Royal Decree of 9 January 2003 requests operators of electronic communications networks and providers of electronic communications services to install a Coordination Cell Justice, individually or jointly, to handle the information requests from Belgian legal authorities.

d) Security requirements for data transfers by communications service providers

The following norms address technical requirements for data transfers by communications service providers.

aa) Format

Article 90*quater* §4 CCP provides that the investigating judge can order persons to make the content that is being or has been transferred accessible in the format he wants.

Article 10*bis* 1° of the Royal Decree of 9 January 2003 provides that the Coordination Cell Justice shall transfer the data to the requesting authority via an easy-to-use form.

Article 10*bis* 2° of the Royal Decree of 9 January 2003 provides that the Minister of Justice and the minister competent for electronic communications shall determine the specific format.

Relevant in this context are the "format requirements" in the ETSI TS 101-331, applicable to data transfers on the basis of Article 6 §3 of the Royal Decree of 9 January 2003 (see section III.B.5.c.bb.):[126]

a) The technical handover interfaces shall provide the results of interception for the entire duration of the interception measure.

---

[126] ETSI TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.10.h, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

NOTE: If a lawful authorization is received during ongoing communication, depending on the intercept implementation, some operational problems might be experienced.

b) These handover interfaces need to be implemented in those telecommunication networks for which the interception capability is required by national laws.

c) The configuration of the handover interface shall ensure that it provides the results of interception.

d) The configuration of the handover interface shall ensure that the quality of service of the telecommunications traffic provided at the handover interface is not inferior to that offered to the target service for each particular call.

e) The configuration of the handover interface shall be such that the transmission to the LEMF of the result of interception provided at the interface can be implemented with standard, generally available transmission paths, protocols and coding principles.

f) Each interception target shall be uniquely associated with a single instance of the handover interface. This could be achieved by separate channels or the use of identifiers.

g) The correlation between the content of communication and intercept related information shall be unique.

h) LEAs require that the format for transmitting the intercepted telecommunications to the monitoring facility be a generally available format.

i) If network operators/service providers/access providers initiate encoding, compression or encryption of telecommunications traffic, LEAs require the network operators/service providers/access providers to provide intercepted telecommunications en clair.

j) LEAs require network operators/service providers/access providers to be able to transmit the intercepted telecommunications to the LEMF via landline or switched connections.

k) The LEMF/LEA will be informed of: 1) the activation of an intercept measure; 2) the deactivation of the intercept measure; 3) any change of the intercept measure; 4) the temporary unavailability of the intercept measure.

bb) Transport channels

Article 10*bis* 1° of the Royal Decree of 9 January 2003 provides that the Coordination Cell Justice shall transfer the data *lege artis* (according to the law of the art), through efficient technical means available on the market.

The ETSI, TS 101-331, applicable to data transfers on the basis of Article 6 §3 of the Royal Decree of 9 January 2003 (see section III.B.5.c.bb.), refers to generally available transmission paths:[127]

> The configuration of the handover interface shall be such that the transmission to the LEMF of the result of interception provided at the interface can be implemented with standard, generally available transmission paths, protocols and coding principles.

---

[127] ETSI TS 101-331, 4.10.e.

cc) Protocol

Article 10*bis* 2° of the Royal Decree of 9 January 2003 provides that the Minister of Justice and the minister competent for electronic communications shall determine the transfer method of data.

Relevant in this context is the reference to "generally available protocols" in ETSI TS 101-331, applicable to data transfers on the basis of Article 6 §3 of the Royal Decree of 9 January 2003 (see section III.B.5.c.bb.):[128]

> The configuration of the handover interface shall be such that the transmission to the LEMF of the result of interception provided at the interface can be implemented with standard, generally available transmission paths, protocols and coding principles.

dd) Time limits

Article 126 §2 of the Electronic Communications Act provides that the operators and services shall immediately transfer the requested data to the requesting authorities.

Article 5 of the Royal Decree of 9 January 2003 provides that the Coordination Cell Justice shall transfer the data in real time to the National Technical & Tactical Support Unit – Central Technical Interception Facility (NTSU-CTIF) after receipt of the warrant pursuant to Article 90*ter* CCP. Article 1 4° of the Royal Decree defines "real time" as the "minimum time necessary for executing a certain performance according to the rules of art, without interruption and with deployment of *adequate means* and personnel" (emphasis added).

Article 6 §1 of the Royal Decree of 9 January 2003 lays down five functional requirements for the data transfer, established in a Council Resolution of 17 January 1995 on the lawful interception of telecommunications.[129] The second functional requirement in Article 6 §1 of the Royal Decree of 9 January 2003 concerns the transfer of interception communications in real time.

Relevant in this context is the reference to "time constraints" in ETSI TS 101-331, applicable to data transfers on the basis of Article 6 §3 of the Royal Decree of 9 January 2003 (see section III.B.5.c.bb.):[130]

> a) A network operator/service provider/access provider shall make the necessary arrangements to fulfil[l] his obligation to enable the interception and delivery of the result of interception from the point in time when the telecommunication installation commences commercial service.
>
> b) The above requirement applies accordingly to the introduction of modifications to the telecommunication installation or to new operational features for existing tele-

---

[128] ETSI TS 101-331, 4.10.e.

[129] Council of the European Union, Council Resolution of 17 January 1995 on the lawful interception of telecommunications, COM 96/C329/01, OJ C 329, 4.11.1996, pp. 1–6.

[130] ETSI TS 101-331, 4.5.

communications services to the extent of their impact on existing interception capabilities.

NOTE 1: It is a national implementation (issue for negotiation) whether the operator does this proactively or passively upon request by the LEA.

c) When a lawful authorization is presented a network operator/service provider/access provider shall co-operate immediately.

NOTE 2: If a lawful authorization is received during an ongoing call, depending on the interception implementation, some operational problems might be experienced.

d) After a lawful authorization has been issued, provision of the results of interception of a target identity shall proceed on a real-time or near real-time basis. In the case of near real-time the LEA should be able to force real-time (by means of emptying any buffers involved) if necessary.

ee) Encryption

The data retention Act of 29 May 2016 added in the Electronic Communications Act an obligation "to provide technological protection measures that make the retained data unreadable for any unauthorized individual from the moment of their registration" (Article 126 §4, 5° of the Electronic Communications Act).

ff) Security measures

Former Article 126 §5 of the Electronic Communications Act (now Article 126 §4) laid down the following technical and security measures for providers and operators:

– to guarantee that the retained data is of the same quality and subject to the same security and protection measures as the network data;
– to implement appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure;
– to ensure that data may be accessed by specially authorized personnel only, i.e., the "Coordination Cell Justice," as provided for in Article 2 of the Royal Decree of 9 January 2003;
– to destroy the data at the end of the applicable data retention period.

The Data Retention Act of 29 May 2016 introduced Article 126 §4 in the Electronic Communications Act, which includes the former Article 126 §5 security measures and the following three new security measures:

– to store the data on the territory of the EU;
– to provide technological protection measures that make the retained data unreadable for any unauthorized individuals from the moment of their registration;
– to subject the use of retained data to an efficient traceability process.

Furthermore, the Data Retention Act of 29 May 2016 also requires the appointment of a data protection officer, to ensure that:

– all data processing made by the Coordination Cell Justice complies with the law;
– the operator or operators concerned collect and retain only the data that may be legally retained;
– only the legally competent authorities have access to the retained data.

Article 6 §1 of the Royal Decree of 9 January 2003 lays down five functional requirements for the data transfer (see section III.B.5.d.dd.). The fifth functional requirement for data transfers provided in Article 6 §1 of the Royal Decree of 9 January 2003 concerns the secure transfer to prevent data interception by third parties.

Article 10*bis* 1° of the Royal Decree of 9 January 2003 provides that the Coordination Cell Justice shall transfer the data via a secure transfer.

Relevant in this context are the "information protection requirements" in the ETSI TS 101-331, applicable to data transfers on the basis of Article 6 §3 of the Royal Decree of 9 January 2003 (see section III.B.5.c.bb.):[131]

> The technical arrangements required within a telecommunication installation to allow implementation of the interception measures shall be realized with due care exercised in operating telecommunication installations, particularly with respect to:
>
> a) the need to protect information on which and how many target identities are or were subject to interception and the periods during which the interception measures were active;
> b) the restriction to a minimum of staff engaged in implementation and operation of the interception measure;
> c) to ensure the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, interception and recording shall be carried out in operating rooms accessible only by authorized personnel;
> d) the result of interception shall be delivered through a handover interface;
> e) no access of any form to the handover interface shall be granted to unauthorized persons;
> f) network operators, service providers and access providers shall take all necessary measures to protect the handover interface against misuse;
> g) the result of interception shall only be transmitted to the LEMF as indicated in the lawful authorization when proof of the authority to receive of the LEMF, and proof of the authority to send of the interface, has been furnished;
> h) authentication and proof of authentication shall be implement subject to national laws and regulations;
> i) if no dedicated routes to the LEMF are used, such proof shall be furnished for each communication set-up;
> j) depending on certain interception cases, LEAs may require confidentiality measures to protect the transmission of the results of such interception. The use of encryption shall be possible;

---

[131] ETSI TS 101-331, 4.5.

k) in order to prevent or trace misuse of the technical functions integrated in the telecommunication installation enabling interception, any activation or application of these functions in relation to a given identity shall be fully recorded, including any activation or application caused by faulty or unauthorized input. The records, which are subject to national regulation, shall cover all or some of:
   1) the target identity of the target service or target services concerned;
   2) the beginning and end of the activation or application of the interception measure;
   3) the LEMF to which the result of interception is routed;
   4) an authenticator suitable to identify the operating staff (including date and time of input);
   5) a reference to the lawful authorization.
l) the network operator/service provider/access provider shall ensure that the records are tamper-proof and only accessible to specific nominated staff.

e) Checks, filtering, and decryption obligations of communication service providers

Under Belgian law, there are no checks and filtering obligations that must be performed (automatically or manually) by Internet providers before or during the execution of the interception process. Of note, however, are the checks and filtering standards set by the ETSI TS 101-331, applicable to data transfers on the basis of Article 6 §3 of the Royal Decree of 9 January 2003 (see section III.B.5.c.bb.):

4.2. General requirements […]

e) The results of interception relating to a target service shall be provided by the network operator, access provider, service provider in such a way that any telecommunications that do not fall within the scope of the lawful authorization shall be excluded by the network operator, access provider, service provider.

NOTE 5: It is assumed that the intercepting system exercises best effort to exclude non-authorized interception patterns (e.g. transferred communication).[132]

4.3. Results of interception

The network operator, access provider or service provider shall, in relation to each target service:

a) provide the content of communication;

b) remove any service coding or encryption which has been applied to the content of communication (i.e., en clair) and the intercept related information at the instigation of the network operator or service provider;

NOTE 1: If coding/encryption cannot be removed through means that are available in the network or service for the given communication, the receiving agencies should be provided with keys, etc. to access the information *en clair*, cf. next clause

[…]

e) intercept related information shall contain:
   1) the identities that have attempted telecommunications with the target identity, successful or not;

---

[132] ETSI TS 101-331, 4.2.

2) identities used by or associated with the target identity;
3) details of services used and their associated parameters;
4) information relating to status;
5) time stamps.[133]

Article 6 §1 of the Royal Decree of 9 January 2003 lays down five functional requirements for the data transfer (see section III.B.5.d.dd.). The third functional requirement for data transfers provided in Article 6 §1 of the Royal Decree of 9 January 2003 concerns the transfer of encrypted information in a generally accessible format.

The fourth functional requirement for data transfers provided in Article 6 §1 of the Royal Decree of 9 January 2003 concerns the transfer of data content in plain language in case the operator of an electronic communications network or the provider of electronic communications introduced encoding, compression, or encryption of the electronic communications traffic. Hence, the transfer takes place without the use of encryption.

6. Formal prerequisites of interception orders

a) Competent authorities

Under normal circumstances, the investigating judge authorizes the monitoring measure (Article 90*ter* §1 CCP).

Article 90*ter* §5, first and second indent CCP provides that

> [i]n a flagrante delicto case and as long as the flagrante delicto situation lasts, "the public prosecutor can order the measure referred to in [Article 90*ter*] paragraph 1 for the criminal offences referred to in article 137 [terrorism criminal offences], 347bis [on crimes regarding the taking of hostages], 434 [unlawful arrest and imprisonment], or 470 [on extortion committed through violence or threats] of the Criminal Code.
>
> Furthermore, in case of flagrante delicto, the public prosecutor can order the measure referred to in paragraph 1 for the criminal offence referred to in Article 137 [terrorism criminal offences] of the Criminal Code, with the exception of the offence referred to in Article 137, § 3, 6° [threat of committing terrorism criminal offences] of the same Code, within seventy-two hours after the discovery of this criminal offence.

Both under normal circumstances, as in the case of *flagrante delicto*, a judicial police officer is designated for the implementation of the measure (Article 90*quater* §1, 5° CCP).

---

[133] ETSI TS 101-331, 4.3.

b) Formal requirements for applications

According to Article 61*quinquies* §1 CCP, the suspect and the civil party have the right to request the investigating judge to perform additional investigation methods.

According to Article 61*quinquies* §2 CCP, the suspect and the civil party shall submit their petition for an additional investigation method in writing to the Registry of the Court of First Instance. The petition must be reasoned and give a detailed description of the requested investigation method.

c) Formal requirements for orders

Article 90*quater* CCP reads as follows:

> §1.For every measure pursuant to article 90ter, a reasoned and written authorization is given in advance by the investigating judge who communicates this to the public prosecutor.
>
> The authorization shall be dated and states:
>
> 1° the indications and the actual facts, specific to the case, which warrant the measure in accordance with article 90ter;
>
> 2° the reasons why the measure is necessary to reveal the truth;
>
> 3° the person, communication means, the computer system or the place that is the subject of the measure;
>
> 4° the period during which the measure can be carried out, which shall not be longer than one month. This period starts on the day of the authorization by which the measure is ordered, or, in case of Article 90quinquies, first paragraph, extended, and runs up to and including the day before the same day of the following month;
>
> 5° the name and capacity of the officer or the judicial police officer designated for the execution of the measure.
>
> In urgent cases, the authorization can be provided verbally. This authorization shall be confirmed no later than within twenty-four hours in the form specified in the second paragraph.

The Act of 5 February 2016 deleted the prescription of this provision under penalty of nullity.[134]

7. Substantive prerequisites of interception orders

a) Degree of suspicion

Article 90*ter* §1 CCP requires serious indications that it concerns an offence referred to in Article 90*ter* §2 CCP, and if the other investigation means are not sufficient to reveal the truth.

---

[134] Act of 5 February 2016 regarding the modification of criminal law and criminal procedure and regarding diverse provisions on criminal policy, *Belgian Official Journal*, 19 February 2016, entry into force on 29 February 2016.

b) Predicate offences

Article 90*ter* §2 CCP provides the following list of offences that can justify a secret interception and secret (network) search:

– 1° Articles 101 to 110 of the Criminal Code [on the attack and conspiracy against the King, the royal family and the government];
– 2° Articles 136*bis* [on genocide], 136ter [on crimes against humanity], 136*quater* [on war crimes], 136*sexies* [on producing, keeping or transporting a tool, a device or any object, and constructing or altering a building to commit, or facilitate the commission of, one of the criminal offences referred to article 136*bis*, 136*ter*, and 136*quater*] and 136*septies* of the same Code [on ordering, proposing, accepting, inciting, attempting to commit one of the criminal offences referred to in article 136*bis*, 136*ter*, and 136*quater*, as well as participating in, and the failure to prevent, the commission of these criminal offences], and Article 41 of the Act of 29 March 2004 regarding the cooperation with the International Criminal Court and the international criminal tribunals [crimes against the administration of justice at the International Criminal Court];
– 3° Book II, Title Iter, of the same Code [terrorism criminal offences];
– 4° Article 147 of the same Code [unlawful arrest and imprisonment by public officials];
– 5° Articles 160 [counterfeiting gold and silver coins], 161 [defacement of gold and silver coins], 162 [counterfeiting coins of another metal; euro coins counterfeiting], 163 [altering such coins], 168 [participation in the issue of, or import on Belgian territory of, counterfeit or defaced coins (or attempt to do so)], 171 [committing fraud in the choice of samples to test the density and weight of gold and silver coins], 173 [counterfeiting or forging government bonds, interest warrants pertaining to such bonds, vouchers, cheques, transfers and banknotes] and 176 [participation in the issue of, or import on Belgian territory of, counterfeit or forged shares, bonds, interest or dividend warrants, or banknotes (or attempt to do so)] of the same Code;
– 6° Articles 180 and 186 of the same Code;

  [– Article 180: counterfeiting or forging state stamps or inspection stamps to hallmark gold or silver; the use of such counterfeit or forged stamps or inspection stamps; counterfeiting or forging coin stamps, moulds (moulds), or other objects or means for the production of the coins; counterfeiting or forging stamps, moulds (moulds), clichés (cast plates) or other objects or means for the production of either stamps, shares, bonds, interest or dividend warrants, bearer banknotes issued by the State Treasury, or banknotes which are legally accepted or whose issuance is permitted by or pursuant to a law or expressed in euros;

  – Article 186: counterfeiting or forging seals, stamps or marks intended for one of the purposes in articles 179 (the national seal) and 180 (see above) of the

Criminal Code, and that belong to foreign States; using such counterfeit or forged seals, stamps or marks; counterfeiting or forging coin stamps, moulds or other objects or means for the production of foreign coins; counterfeiting or forging stamps, moulds, clichés (cast plates) or other objects or means for the production of bearer banknotes issued by a foreign State, or banknotes which are legally accepted there or whose issuance is permitted by a law of a foreign State or by a provision that has force of law there; counterfeiting the seal, stamp or mark of a foreign government (or attempt to do so); using such counterfeit or forged seals, stamps or marks (or attempt to do so)];

- 7° Article 210*bis* of the same Code [forgery through entering, altering or deleting computer data or through altering their potential use, thereby changing the legal scope of such data];
- 8° Articles 246, 247, 248, 249, and 250 of the same Code [on the bribery of persons exercising a public function];
- 9° Article 259*bis* of the same Code [on the prohibition for public officials: 1° to unlawfully intercept, take cognizance and record non-publicly accessible communication; 2° to possess, reveal or disseminate to another person, or knowingly make use of, the content of non-publicly accessible communication or data from a computer system that has been unlawfully intercepted or recorded or of which unlawful cognizance has been taken];
- 10° Article 314*bis* of the same Code [on the prohibition, applicable to everyone: 1° to unlawfully intercept, take cognizance and record non-publicly accessible communication; 2° to possess, reveal or disseminate to another person, or knowingly make use of, the content of non-publicly accessible communication or data from a computer system that has been unlawfully intercepted or recorded or of which unlawful cognizance has been taken];
- 11° Articles 324*bis* and 324*ter* of the same Code [on criminal organisations];
- 12° Articles 327, 328, 329 or 330 of the same Code [on threating to attack persons or property and giving false information on serious attacks], to the extent that a complaint has been filed;
- 13° Article 331*bis* of the same Code [on 1° threatening to use radioactive materials or instruments, with the intent to cause death or serious injury to a person, or to cause significant damage to goods or to the environment; with the same intent, threatening to commit an act against a nuclear installation or to disrupt the operation of such an installation; 2° threatening to commit theft of nuclear material in order to force a natural person or a legal person, an international organization or a State to do or omit something; 3° threatening to use biological or chemical weapons or products for an attack on persons, on property, on legal persons, on international organizations or on a State.];
- 14° Article 347*bis* of the same Code [on criminal offences regarding the taking of hostages];

15° Articles 372 to 377bis of the same Code;

[– Article 372: sexual assault, without violence or threat, against or with the help of children below the full age of sixteen;

– Article 373: sexual assault, with violence, coercion, threat or ruse, or made possible by a handicap, physical or mental disability of the victim;

– Article 374: on assault;

– Articles 375, 376 and 377: on rape;

– Article 377*bis*: voyeurism, sexual assault and rape, when one of the motives of the criminal offence is hatred, disdain or hostility to a person based on race, color, ancestry, national or ethnic origin, nationality, sex, sexual orientation, marital status, birth, age, fortune, religion or philosophy of life, current or future health status, disability, language, political conviction, unionism, physical or genetic trait or social origin];

– 16° Article 377*quater* of the same Code [the adult who, through information and communications technology, proposes to a minor under the age of sixteen to meet with the intention of committing a criminal offence referred to Chapter V (voyeurism, sexual assault and rape), chapters VI (decay of youth and prostitution) and VII (sex offences: displaying, distributing or selling pamphlets or other writings, whether or not printed, images or prints, emblems or objects, that are contrary to accepted principles of morality; singing, reading, reciting or expressing obscenity/ribaldry; by displaying, distributing or selling writings, whether or not printed, or by any other means of publicity, recommending the use of any means of abortion, providing instructions on the manner to purchase or use them, or recommending persons who apply them; trading in abortion tools and instruments; displaying, sharing, trading, acquiring, accessing through information and communications technology or possessing child pornographic material), to the extent that this proposal has been followed by material actions leading to such a meeting];

– 17° Articles 379, 380 [on the fornication, moral decay or prostitution of minors] and 383*bis*, §§ 1 [displaying, sharing and trading child pornographic material] and 3 [the criminal offence in Article 383bis §1 concerns an act of participation in the main or ancillary activity of an association], of the same Code;

– 18° Article 393 of the same Code [on manslaughter];

– 19° Articles 394 [on murder] or 397 [on intoxication] of the same Code;

– 20° Articles 428 and 429 of the same Code [on kidnapping of minors];

– 21° Article 433*bis*/1 of the same Code [the adult who communicates with an apparent or presumed minor through information and communications technologies in order to facilitate the commission of a criminal offence against him: 1° if he has concealed, or lied about, his identity, age and capacity; 2° if he has emphasized the discretion to be observed regarding their conversations; 3° if he has offered any gift or advantage; 4° if he has used any other trick];

- 22° Articles 433*quinquies* to 433*octies* of the same Code [in case of human trafficking: the exploitation of prostitution or other forms of sexual exploitation; the exploitation of begging; inhuman working conditions; removal or organs or human body material; causing a person to commit a criminal offence against his will. Attempt to commit this criminal offence is also punishable].
- 23° Article 434 of the same Code [on unlawful arrest and imprisonment];
- 24° Articles 468, 470, 471 or 472 of the same Code [on theft committed through violence or threats, and extortion];
- 25° Article 475 of the same Code [on manslaughter to facilitate or ensure the impunity of theft or extortion];
- 26° Book II, title IX, chapter I, section IIbis [on the theft and extortion of nuclear materials], and chapter Ibis [on the external protection of nuclear material and other radioactive material] of the same Code;
- 27° Articles 504*bis* and 504*ter* of the same Code [on private commercial bribery];
- 28° Article 504*quater* of the same Code [on computer fraud].
- 29° Article 505, first paragraph, 1° of the same Code [on possession of stolen goods, embezzled goods, or goods that have been acquired by a criminal offence] when the items in question were stolen, embezzled or acquired by a crime or misdemeanour referred to in that article;
- 30° Article 505, first paragraph, 2°, 3° and 4° of the same Code [on specific transactions of stolen goods, embezzled goods, or goods that have been acquired by a criminal offence];
- 31° Articles 510, 511, first paragraph and 516 of the same Code [on arson];
- 32° Article 520 of the same Code [on the destruction of constructions by causing an explosion], if there is totality of the circumstances referred to in Articles 510 or 511, first paragraph, of the same Code;
- 33° Articles 550*bis* [on hacking] and 550*ter* [on data and system interference] of the same Code;
- 34° Article 2*bis* of the Act of 24 February 1921 concerning the trafficking of poisonous, narcotic, stupefying, psychotropic, disinfectant and antiseptic substances and those substances which may be used to make illicit narcotic or psychotropic substances [on criminal offences regarding narcotics or stupefying substances, other psychotropic substances that may cause dependency, and cultivating plants to extract these substances];
- 35° The Act of 28 May 1956 on explosives and the deflagration substances and mixtures and thereby loaded vehicles;
- 36° Article 1 of the Royal Decree of 12 April 1974 regarding certain actions relating to materials with a hormonal, anti-hormonal, anabolic, beta-adrenergic, anti-infectious, anti-parasitic and anti-inflammatory effect, which relate to criminal

offences criminalized by the Act of 24 February 1921 concerning the trafficking of poisonous, narcotic, stupefying, psychotropic, disinfectant and antiseptic substances [on the licence for the actions relating to these materials];

- 37° Articles 77*bis* to 77*quinquies* of the Act of 15 December 1980 on access to the territory, residence, establishment and removal of foreigners [on human trafficking contributing to the entry, travel or stay by a non-EU national in the territory of a Member State of the EU or a State party to an international agreement on the crossing of the external borders, this in violation of the legislation of this State, with a view to obtaining a capital gain directly or indirectly];
- 38° Article 10, § 1, 2° of the Act of 15 July 1985 regarding the use in animals of substances with hormonal, anti-hormonal, beta-adrenergic or production stimulating effects [on the offences relating to the administration of such substances, and the trade in animals to which such substances were unlawfully administered];
- 39° Article 10 of the Act of 5 August 1991 on the import, export and transit of arms, ammunition and materials specifically intended for military use and the associated technology [on illegal trade in weapons, ammunition and materials specifically intended for military use, and the associated technology].
- 40° Article 145 §3 [on fraudulently establishing electronic communications through an electronic communications network, in order to provide oneself or another person an unlawful benefit] and § 3bis [on the use of an electronic communications network or provider, or of other electronic communication means, to cause nuisance to his correspondent or to cause harm, or setting up a device intended to commit the previous offences] of the Act of 13 June 2005 on electronic communications;
- 41° Articles 8 to 11, 14, 16, 19, 1°, 2°, 3°, 5° and 6°, 20, 22, 27 and 33 of the Act of 8 June 2006 on the regulation of economic and individual activities with weapons, also called the "Arms Act;"
- 42° Articles 21 to 26 of the Cooperation Agreement between the Federal State, the Flemish Region, the Walloon Region and the Brussels Capital Region concerning the implementation of the Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction, Paris 13 January 1993;
- 43° Article 47 of the Decree of the Flemish Parliament of 15 June 2012 on the import, export, transit and transfer of defence-related products, other material for military use, law enforcement equipment, civilian firearms, parts and ammunition;
- 44° Article 20 of the Decree of the Walloon Region of 21 June 2012 on the import, export, transit and transfer of civil weapons and defence-related products;
- 45° Article 42 of the Ordonnance of the Brussels Capital Region of 20 June 2013 on the import, export, transit and transfer of defence-related products, other ma-

terial for military use, law enforcement equipment, civilian firearms, parts, accessories and its ammunition;

Article 90*ter* §4 CCP provides that:

> [a] criminal offence, referred to in Articles 322 or 323 of the Criminal Code [on associations with a view to commit an attack on persons or property] can also warrant a measure, to the extent that the association is formed with the aim to commit an attack against the persons or properties referred to in § 2, or to commit the criminal offence referred to in article 467, first paragraph, of the Criminal Code [on theft though burglary, climbing through, or false keys, or by a public official through his ministry]

The potential or the likely sentencing range for the offences listed in Article 90*ter* §§2 and 4 does not serve as additional mitigating criteria.

c) Persons and connections under surveillance

Article 90*ter* §1, fourth indent CCP provides that the interception measure "can only be ordered to trace the data that can serve to reveal the truth. The measure can only be ordered in respect of persons suspected of having committed the criminal offence on the basis of precise facts, in respect of communication means or computer systems frequently used by a suspected person or in respect of the places where he is suspected to stay. The measure can also be ordered in respect of persons who are suspected on the basis of precise facts to be in regular contact with a suspected person."

The parliamentary preparatory works specify that proactive monitoring is prohibited (see section I.A.2.b.), for instance, in relation to a reputed criminal: the application of Article 90*ter* CCP requires suspicion.[135]

d) Principle of subsidiarity

According to Article 90*ter* §1, second indent CCP, the investigating judge may only carry out an interception measure if the other investigation means are not sufficient to reveal the truth. The parliamentary preparatory works note that prior unsuccessful application of the other investigation methods by the investigating judge is not required: it suffices that the investigating judge considers that the other measures are unlikely to be successful.[136]

---

[135] Parliamentary preparatory works, Belgian Senate, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, 1992-1993, 1 September 1993, no. 843-1, p. 15, available at http://www.senate.be/lexdocs/S0539/S05390297.pdf

[136] *Ibid.*, p. 14.

e) Proportionality of interception in individual cases

The investigating judge is obliged to verify that the interception is proportionate to the seriousness of the offence in the individual case. According to Article 90*ter* §1, second indent CCP, the investigating judge may intercept only in exceptional cases.

Van den Wyngaert relates the proportionality principle to the list of offences that can justify an interception measure (Article 90*ter* §2 CCP; see section III.B.7.b.).[137] Hence, interception measures for offences other than those listed in Article 90*ter* §2 violate the principle of proportionality.

There is no requirement that the anticipated evidence will likely be obtained by means of the interception measure.

f) Consent by a communication participant to the measure

As noted (section III.B.6.b.), according to Article 61*quinquies* §3 CCP, the judge may reject the request by the suspect or a civil party to perform additional investigation methods, if he considers the measures unnecessary in order to reveal the truth or if, at that moment, he considers the measures prejudicial to the investigation. Hence, the consent by a communication participant to the measure is not a decisive prerequisite for the interception order.

8. Validity of interception order

a) Maximum length of interception order

Article 90*quater* §1, 4° CCP provides that "the period during which the measure can be carried out, which shall not be longer than one month. This period starts on the day of the authorization by which the measure is ordered, or, in case of Article 90quinquies, first paragraph, extended, and runs up to and including the day before the same day of the following month."

b) Prolongation of authorization

In both normal circumstances and cases of emergency, Article 90*quinquies* CCP allows prolongation of the interception warrant:

> The investigating judge can prolong the operation of the authorization referred to in Article 90quater, § 1, one or more times with a term that may not be longer than one month, with a maximum of six months, without prejudice to his decision to terminate the measure as soon as the circumstances that justified the measure have disappeared.

---

[137] Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, p. 983.

> This period of six months starts on the day of the first authorization by which the measure is ordered and runs up to and including the day before the same day of the sixth following month. If, because of its technical preparation, the measure was actually started on a later date than that of the first authorization, the six-month period shall start on the day of that actual start and at the latest two months after the date of the first authorization.
>
> The provisions referred to in Article 90quater, § 1, apply to the prolongation referred to in the previous paragraph. The authorization also mentions the precise circumstances that warrant the prolongation of the measure.

Hence, the prolongation of the monitoring measure follows the same procedure as the initial application for an interception measure.

c) Revocation of authorization

In both normal circumstances and cases of emergency, Article 90*quinquies* §1, first indent CCP allows revocation of the monitoring warrant:

> The investigating judge can prolong the operation of the authorization referred to in Article 90quater, § 1, one or more times with a term that may not be longer than one month, with a maximum of six months, without prejudice to his decision to terminate the measure as soon as the circumstances that justified the measure have disappeared. […]

Freyne holds that the investigating judge has a duty to revoke the authorization during the monitoring measure in case it becomes apparent that other investigation methods are sufficient to reveal the truth (principle of subsidiarity, see section III.B.7.d.).[138]

9. Duties to record, report, and destroy

a) Duty to record and report

First, Article 90*quater* §3 *in fine* CCP provides that "[t]he designated judicial police officers shall report in writing to the investigating judge about the execution of the authorization at least every five days."

Second, Article 90*sexies* §1 CCP lays down reporting requirements regarding the interception measure:

> §1. The designated judicial police officers make available to the investigating judge:
>
> 1° the file containing the recorded non-public communication or data from a computer system obtained as a result of the measures taken in application of the articles 90ter, 90quater and 90quinquies;

---

[138] Thierry Freyne, "De bewaking van privécommunicatie en -telecommunicatie in strafonderzoeken: een stand van zaken" (The monitoring of private communications and telecommunications in criminal proceedings: a state of affairs), *Tijdschrift voor Strafrecht*, 2008, vol. 3, p. 173, no. 18.

> 2° the transcription or minutes of the parts of recorded communications or data that the designated police officers deem relevant for the investigation, and any translation thereof;
>
> 3° if applicable, the location of the data referred to in the provision under 2° in the computer system;
>
> 4° a general description of the content and the identification data of the communication means or computer systems used with regard to the communication or data that are not deemed relevant.

According to Article 90*septies* §3 CCP, the files and documents mentioned in Article 90*sexies* §1 CCP do not necessarily need to be recorded in an official record (see section III.B.9.b.).

Third, Article 90*septies* § 2 CCP provides that "[e]ach file contains the subject of the recorded non-publicly accessible communication or data of a computer system and the days and hours on which the measure was executed."

b) Duty to destroy

With regard to the interception measure by the Belgian investigating judge, Article 90*septies* §3 CCP reads as follows:

> Any note in the context of the execution of the measures referred to in articles 90ter, 90quater and 90quinquies by the persons designated for this purpose, which is not recorded in an official report, shall be destroyed with the exception of the provisions in article 90sexies, § 1, 2°, 3° and 4° [see section III.B.9.a.] and without prejudice to article 33 of the Act of 25 December 2016 containing various amendments to the Code of Criminal Procedure and the Criminal Code, with a view to the improvement of the special investigation methods and certain investigation methods with respect to the internet and electronic and telecommunications and establishing a database of voice prints. The judicial police officers designated for the execution of the measure proceed to this destruction and state this in an official report.

Article 90*ter* §6 CCP allows under certain conditions the interception by competent foreign authorities, if the person to whom this measure applies is located on the Belgian territory. Article 90*ter* §7 *in fine* CCP provides that:

> [i]n case the investigating judge does not allow the measure referred to in § 6, he shall also notify the foreign government that the gathered data must be destroyed and cannot be used.

10. Notification duties and remedies

a) Duty to notify persons affected by the measure

Article 90*novies* CCP lays down a notification duty concerning any person subject to a monitoring measure:

> No later than fifteen days after the decision on the settlement of the administration of justice has become final or after the summons referred to in Article 524bis, § 6, has been deposited at the Registry of the court or of the court of appeal, the registrar shall, at the request of the public prosecutor or where appropriate, of the Attorney General, notify, in

writing, any person in respect of whom a measure referred to in Article 90ter has been taken of the nature of that measure and of the days on which it was executed, unless his identity or domicile cannot reasonably be ascertained.

Arnou notes that the duty of notification of the nature of measure and the days on which it was executed is not prescribed under sanction of nullity (see below, section IV.2.),[139] nor do the parliamentary preparatory works provide any clarity in this regard. In any case, no exclusion will follow on the basis of an alleged violation of the rights of defence because, as noted, the suspect (not third parties) has access to the judicial file on the basis of Article 61*ter* CCP. Arnou adds that, at most, a disciplinary sanction or civil sanction will be allowed.[140]

Unfortunately, the Board of Public Prosecutors could not positively respond to our request of 2 April 2015 for data on infringements of the law on interception of telecommunications. Hence, we are unable to report on notification practices.

b) Remedies

Article 90*ter* CCP and following are silent regarding the remedies available to the suspect during the interception. Therefore, the general rules of criminal procedure apply as regards the remedies that are available to a person who becomes aware that they were subject to an illegally performed interception measure. As noted (see section II.A.3.), the Courts in Chambers (court of instruction in first instance) and the Chamber of Indictment (court of instruction in appeal) evaluate the legality of the evidence collection during the investigation phase (Article 131 CCP, Article 135 §2 CCP, and Article 235*bis* §6 CCP). Both the Courts in Chambers and the Chamber of Indictment determine the grounds for finding a nullity on the basis of the so-called Antigoon criteria (see below, section IV.2.). The lack of reasoning by the Courts in Chambers and the Chamber of Indictment may give rise to appeal before the Chamber of Indictment (Article 135 §2 CCP) respectively the Supreme Court (Article 235*bis* §6 CCP *versus* Article 416 CCP). The proceedings before the Courts in Chambers and the Chamber of Indictment are public and adversarial (Article 127 §4 CCP, respectively Article 135 §3 CCP).

It is of note that illegally obtained files are not destroyed but instead removed from the judicial file and kept at the Registry of the Court of First Instance (Article 235*bis* §6 CCP). The Indictment Chamber decides who can have access to the removed files in light of the right of defence. In this regard, the Supreme Court also

---

[139] Legal experts confirmed that the notification duty is never respected, because it is not prescribed under sanction of nullity.

[140] Luc Arnou, "Afluisteren tijdens het gerechtelijk onderzoek" (Wiretapping during the investigation); in Commentaar Strafrecht en strafvordering (Commentary criminal law and criminal procedural law), Gent, Kluwer, 2008, vol. 59, pp. 80–81, no. 83.

held that the trial judge may allow parties access to the removed documents that are essential for the right of defence.[141]

c) Criminal consequences of unlawful interception measures

As noted, the interception measure in Article 90*ter* CCP provides an exception to the general prohibition of the interception of (tele-)communications (Article 314*bis* CC and Article 259*bis* CC, see section II.A.4.a.). Unlawful interception measures could thus theoretically entail criminal responsibility.

However, the Board of Public Prosecutors could not positively respond to our request of 2 April 2015 for data on the infringements of the law on interception of telecommunications. Hence, we are unable to list specific sanctions imposed on officials for wrongfully conducting an interception measure, nor to provide the frequency with which such cases occur or sanctions are imposed.

As noted earlier (section III.B.10.a.), at most, a disciplinary sanction or civil sanction would be allowed for violations of the notification duty towards persons affected by the measure.

11. Confidentiality requirements

a) Obligations of telecommunications service providers to maintain secrecy

As noted (section III.B.5.b.), Article 90*quater* §§2, 4 CCP lay down cooperation duties for individuals and the private sector. Both provisions include confidentiality requirements.

b) Sanctions against telecommunications service providers and their employees

Article 90*quater* §§2, 4 CCP lay down specific sanctions for infringements of their obligations.

Article 90*quater* §2, third and fourth indents CCP read as follows:

> Any person, who by virtue of his office is informed of the measure or cooperates thereto, is bound by secrecy. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code.
>
> Any person who refuses technical cooperation to the requests referred to in the first paragraph, or who does not grant such cooperation in real time or, where applicable, at the time specified in the request, cooperation of which the further rules shall be determined by the King, on the proposal of the minister of Justice and the minister competent for Telecommunications, shall be punished by a fine of twenty-six euros to twenty-thousand euros.

---

[141] Supreme Court, 18 February 2003, P020913N.

Article 90*quater* §4, third and fourth indents CCP read as follows:

> Any person who refuses to cooperate with the requests referred to in paragraphs 1 and 2 shall be punished with imprisonment of six months to one year and by a fine of twenty-six euros to twenty thousand euros or with one of these penalties only.
>
> Any person, who by virtue of his office is informed of the measure or who is requested to grant technical cooperation is bound by secrecy. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code.

A circular of the Board of Prosecutors General of 17 December 2009 explains the criminal policy regarding violations of the cooperation duties under Article 46*bis* §2 CCP (collection of identification data of electronic communications), Article 88*bis* §2 CCP (tracing of traffic data, and localization of electronic communications), and Article 90*quater* §2 CCP.[142] Investigations are possible in case of manifest refusals to cooperate. In other cases, the reaction will depend on the seriousness of the infringement or the specific circumstances.

No specific sanctions are foreseen for violations of the security requirements for data transfers by communications service providers (section III.B.5.d.).

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

a) Collection of traffic data

aa) Relevant information

Article 88*bis* CCP refers to the tracing of traffic data, and localization of electronic communications. Article 88*bis* §1 CCP describes the relevant information:

1° trace the traffic data of electronic communication means from or to which electronic communications are or were made;

2° locate the origin or destination of electronic communications.

Article 88*bis* §1 CCP lays down the prerequisites for the tracing of traffic data, and localization of electronic communications:

> §1. When there are serious indications that the criminal offences could result in a correctional main sentence of one-year imprisonment or a more severe penalty, and the investigating judge considers that there are circumstances that necessitate the detection of electronic communications or the localization of the origin or the destination of electronic communications in order to reveal the truth, he can:
>
> […]

---

[142] Board of Prosecutors General, "Telecommunicatierichtlijn inzake het opsporings- en vervolgingsbeleid betreffende inbreuken op de medewerkingsverplichtingen vervat in de artikelen 46bis § 2, 88bis § 2 en 90quater § 2 van het wetboek van strafvordering" (Telecommunications Circular regarding the investigation and prosecution of violations of the cooperation duties under Articles 46*bis* §2, 88*bis* §2 and 90*quater* §2 CCP), COL 14/2009, 17 December 2009, available (in Dutch and French) at https://www.om-mp.be/

In the cases referred to in the first paragraph, for every electronic communication means of which traffic data are traced or for which the origin or destination of the electronic communications are located, the day, time, duration, and, if necessary, the location of the electronic communication means shall be determined and included in an official record.

In a reasoned warrant, the investigating judge shall state the factual circumstances of the case that warrant the measure, the proportionality with regard to privacy and the subsidiarity in relation to any other investigatory act.

He shall also state the duration of the measure for the future, which cannot be longer than two months from the warrant, without prejudice to a renewal and, where applicable, the past period on which the request extends in accordance with paragraph 2.

In case of flagrante delicto, the public prosecutor can order the measure for the criminal offences referred to Article 90ter, §§ 2, 3 and 4. In that case, the measure must be confirmed by the investigating judge within twenty-four hours.

However, if it concerns the criminal offence referred to in Article 137 [terrorism criminal offences], 347bis [taking of hostages], 434 [unlawful arrest and imprisonment] or 470 [extortion by force] of the Criminal Code, with the exception of the criminal offence referred to in Article 137, § 3, 6 ° [threat of committing terrorism criminal offences] of the same Code, the public prosecutor can order the measure as long as the flagrante delicto situation lasts, without the need for a confirmation by the investigating judge.

If it concerns the criminal offence referred to in Article 137 of the Criminal Code, with the exception of the offence referred to in Article 137, § 3, 6 °, of the same Code, the public prosecutor can also order the measure within seventy-two hours after the discovery of this criminal offence, without the need for a confirmation by the investigating judge.

The public prosecutor can, however, order the measure upon request of the complainant, if this measure appears to be indispensable for establishing a criminal offence referred to in Article 145, § 3 and § 3bis of the Act of 13 June 2005 on electronic communications.[143]

In urgent cases, the measure can be ordered verbally. The order must be confirmed as soon as possible in the form specified in the fourth and fifth paragraphs.

bb) Duty of addressees to disclose information in manual procedures

Article 88*bis* §1, second indent CCP, provides:

[…] he [the investigating judge] can, if necessary, request, directly or through the police service designated by the King, the cooperation of:

– the operator of an electronic communications network, and

---

[143] Article 145 §3, 1° of the Act of 13 June 2005 on electronic communications punishes anyone who carries out fraudulent electronic communications through a network of electronic communication in order to gain for himself/herself or another an unlawful advantage; Article 145 §3*bis* of the Act of 13 June 2005 on electronic communications incriminates "the person who uses an electronic communications network or an electronic communications service or other electronic means to annoy or cause damage to his correspondent and the person installing any device intended to commit the offence and the attempt to commit it."

– anyone who, within the Belgian territory, makes available or offers, in whatever way, a service consisting of the transmission of signals via electronic communications networks, or that enables users to obtain, receive or distribute information via an electronic communications network. This also includes the provider of an electronic communications service.[144]

Article 88*bis* §4 CCP reads as follows:

The actors referred to in § 1, second paragraph, provide the requested data in real time or, where applicable, at the time determined in the request, according to the further rules established by the King, on the proposal of the minister of Justice and the minister competent for Telecommunications.

Any person, who by virtue of his office is informed of the measure or cooperates thereto, is bound by secrecy. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code.

Any person who refuses technical cooperation to the requests referred to in this article, or who does not grant such cooperation in real time or, where applicable, at the time specified in the request, cooperation of which the further rules shall be determined by the King, on the proposal of the minister of Justice and the minister competent for Telecommunications, shall be punished by a fine of twenty-six euros to ten thousand euros.

The modalities of the cooperation duties under Article 88*bis* CCP are laid down in the Royal Decree of 9 January 2003. Article 4 of the Royal Decree provides that the traffic data of telecommunications, meaning to or from where calls are or were made and that are more than 30 days old, shall be provided as soon as they are available and, at the latest, on the next working day at the same hour as the receipt of the request, unless the request provides otherwise.

No automated procedure is prescribed for data transfers under Article 88*bis* CCP.

Also relevant in the context of Article 88*bis* CCP are the duties to provide a technical and organizational infrastructure (section III.B.5.c.), the security requirements for data transfers by communications service providers (section III.B.5.d.), and the checks, filtering, and decryption obligations of communications service providers (section III.B.5.e.).

b) Collection of subscriber data

aa) Relevant information

Article 46*bis* CCP is on the collection of identification data of electronic communications. Article 46*bis*, §1, 1° and 2° CCP describes the relevant information:

---

[144] See also on Article 46*bis* CCP (identification data), Article 90*quater* CCP (secret interception and secret (network) search) and Article 464/1 CCP (criminal enforcement investigation): This definition corresponds to the autonomous (broad) interpretation by the Belgian Supreme Court of the term "electronic communications provider" in Article 46*bis* CCP (judgment of 18 January 2011 P.10.1347.N, available via http://jure.juridat.just.fgov.be/).

1° the identification of the subscriber or the habitual user of a service referred to in the second paragraph, second indent, or of the electronic communication means used;

2° the identification of the services referred to in the second paragraph, second indent, on which a specific person is subscribed or that are habitually used by a specific person.

bb) Substantive prerequisites of collection

(1) Degree of suspicion

According to Article 46*bis* §1 CCP, the public prosecutor may proceed or cause to proceed with the collection of identification data of electronic communications "on the basis of any information held in his possession possession or through access to the customer files of the actors referred to in the second paragraph" [the operator of an electronic communications network, and electronic communications providers; see section III.C.1.b.dd.].

(2) Predicate offences

Article 46*bis* CCP does not contain a list of offences that can justify the measure. According to Article 46*bis* §1 CCP, the measure can only be ordered for crimes and misdemeanours; hence, *a contrario*, not for contraventions.

(3) Persons and connections under surveillance

Article 46*bis* §1, 1° CCP mentions the possibility to identify "the subscriber or the habitual user of a service referred to in the second paragraph, second indent [see section III.C.1.b.dd.], or of the electronic communication means used."

Article 46*bis* §1, 2° CCP mentions the possible to identify "the services referred to in the second paragraph, second indent [see section III.C.1.b.dd.], on which a specific person is subscribed or that are habitually used by a specific person."

(4) Principle of subsidiarity

Article 46*bis* §1, third indent CCP provides that the warrant respects subsidiarity in relation to any other investigatory act.

(5) Proportionality of interception in individual cases

Article 46*bis* §1, third indent CCP provides that the warrant respects proportionality in relation to privacy.

(6) Consent by a communication participant to the measure

As noted (section III.B.6.b.), according to Article 61*quinquies* §3 CCP, the judge may reject the request by the suspect or a civil party if he considers the measures unnecessary in order to reveal the truth or if, at that moment, he considers the measures prejudicial to the investigation. Hence, the consent by a communication participant to the measure is not a decisive prerequisite for the interception order.

cc) Formal prerequisites of collection

(1) Competent authorities

The public prosecutor authorizes the measure (Article 46*bis* §1, first indent CCP). He can, if necessary, request, directly or through the police service designated by the King, the cooperation of:

– the operator of an electronic communications network, and

– anyone who, within the Belgian territory, makes available or offers, in whatever way, a service consisting of the transmission of signals via electronic communications networks, or that enables users to obtain, receive or distribute information via an electronic communications network. This also includes the provider of an electronic communications service (Article 46*bis* §1, second indent CCP).

(2) Formal requirements for applications

Section III.B.6.b. discusses the right of the suspect and a civil party to request the investigating judge to carry out additional investigation methods.

(3) Formal requirements for orders

Article 46*bis* §1 CCP provides that the public prosecutor issues a reasoned and written decision in order to proceed or cause to proceed to the collection of identification data.

Article 46*bis* §1 *in fine* CCP reads as follows:

> For criminal offences that cannot result in a correctional main sentence of one-year imprisonment or a more severe penalty, the public prosecutor can only request the data referred to in the first paragraph for a period of six months prior to his decision.

dd) Duty of addressees to disclose information

Article 46*bis* §1, second indent CCP reads as follows

> […] he [the public prosecutor] can, if necessary, request, directly or through the police service designated by the King, the cooperation of:

– the operator of an electronic communications network, and

– anyone who, within the Belgian territory, makes available or offers, in whatever way, a service consisting of the transmission of signals via electronic communications networks, or that enables users to obtain, receive or distribute information via an electronic communications network. This also includes the provider of an electronic communications service.

This definition corresponds to the autonomous (broad) interpretation by the Belgian Supreme Court of the term "electronic communications provider" in Article 46*bis* CCP. In the so-called *Yahoo!* case, the public prosecutor fined the US-based company Yahoo! for refusing to hand over an IP-address and information regarding the suspect's Yahoo! account. Yahoo! argued that the data was located on US soil and that sharing such data with foreign authorities would infringe US privacy law. Yahoo! considered that Belgian authorities should rely on MLA instead of direct cooperation requests.

On 18 January 2011, the Belgian Supreme Court held that the obligation to cooperate under Article 46*bis* CCP is not limited to electronic communications providers under the Act of 13 June 2005 on electronic communications,[145] which implements the EU directives on electronic communications, including Directive 2002/21/EC of 7 March 2002.[146] In its judgment of 18 January 2011, the Supreme Court held that:

> the obligation to cooperate under article 46bis of the Code of Criminal Procedure […] also applies to anyone who provides a service, which consists wholly, or mainly in the conveyance of signals on electronic communications networks. The person who provides a service which consists of enabling its customers to obtain, or to receive or distribute information through an electronic network, can also be a provider of an electronic communications service.[147]

On 1 December 2015, in its third decision in the *Yahoo!* case, the Belgian Supreme Court ruled that Yahoo!'s economic activities on Belgian soil (advertisement in the three national languages, special mail box for Belgian consumers) implied a duty to respect Belgian law and therefore also a duty to cooperate with Belgian authorities.[148]

Of note is that, on 23 February 2018, the Court of Appeal of Brussels lodged a request for preliminary ruling by the Court of Justice of the EU, inquiring whether

---

[145] Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 20 June 2005, entry into force on 30 June 2005.

[146] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ 2002 L 108, p. 33).

[147] Supreme Court, 18 January 2011, P.10.1347.N, available via http://jure.juridat.just.fgov.be/

[148] Supreme Court, 1 December 2015, P.13.2082.N, available via http://jure.juridat.just.fgov.be/

Skype can be considered as an electronic communications provider under Directive 2002/21/EC of 7 March 2002[149] (see the explanatory note, on Article 46*bis* and Article 90*quater* CCP).

Article 46*bis* §2 CCP reads as follows:

> The actors referred to in § 1, second paragraph, first and second indents, from whom the data referred to in paragraph 1 is requested, provide the public prosecutor or the judicial police officer with the data in real time or, where applicable, at the time determined in the request, according to the further rules established by the King, on the proposal of the minister of Justice and the minister competent for Telecommunications.
>
> The King determines, upon advice from the Commission for the protection of privacy and on the proposal of the minister of Justice and the minister competent for Telecommunications, the technical conditions for access to the data referred to in § 1, which are available for the public prosecutor and for the police service designated in the same paragraph.
>
> Any person, who by virtue of his office is informed of the measure or cooperates thereto, is bound by secrecy. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code.
>
> Any person who refuses to communicate the data or does not communicate it in real time or, where applicable, at the time specified in the request, shall be punished by a fine of twenty-six euros to ten thousand euros.

ee) Automated procedure of disclosure

The modalities of the cooperation duties under Article 46*bis* CCP are laid down in the Royal Decree of 9 January 2003.

Article 3 §2 of the Royal Decree prescribes an automated procedure of disclosure for electronic communications networks that were granted numbering capacity in the national numbering plan (NNP).[150] The access is granted via a secure Internet application, by means of which the operator receives a request, which he is required to process and reply to immediately. The National Technical & Tactical Support Unit – Central Technical Interception Facility (NTSU-CTIF) determines further technical details of the procedure and shall only consult the database after receipt of a request based on Article 46*bis* CCP. The NTSU-CTIF shall keep a log

---

[149] Request for a preliminary ruling from the Cour d'appel de Bruxelles (Belgium) lodged on 23 February 2018 – Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (IBPT), Case C-142/18, available via http://curia.europa.eu

[150] The Belgian Institute for Postal Services and Telecommunications (BIPT) grants numbering capacity on the basis of Article 11 §1 of the Electronic Communications Act of 13 June 2005; a telephone numbering plan is a common example of NNP, used to assign telephone numbers to telephony endpoints such as subscriber telephones. For more information on NPP, see the website of the International Telecommunication Union (ITU): https://www.itu.int/oth/T0202.aspx?parent=T0202

file of every access to and consultation of the database and take the necessary physical and software-based measures in order to provide an adequate security level.

Article 3 §1 of the Royal Decree provides that the Coordination Cell Justice of the operators of electronic communications networks that were not granted numbering capacity in the NNP, and the electronic communications providers shall communicate in real time according to the rules provided in Article 10*bis* of the same Royal Decree (see section III.B.5.d. and e.).

Also relevant in the context of Article 46*bis* CCP are the duties to provide a technical and organizational infrastructure (section III.B.5.c.), the security requirements for data transfers by communications service providers (section III.B.5.d.), and the checks, filtering, and decryption obligations of communications service providers (section III.B.5.e.).

c) Data retention[151]

As noted (section I.A.2.a.dd), the general data retention provision is Article 126 of the Electronic Communications Act. However, on 11 June 2015, the Belgian Constitutional Court invalidated Article 126 of the Electronic Communications Act.[152] A new Belgian data retention Act of 29 May 2016 entered into force on 28 July 2016. As noted (section I.A.2.dd), on 19 July 2018, the Constitutional Court of Belgium requested a preliminary ruling from the Court of Justice of the European Union (CJEU), regarding the compatibility of the Belgian general data retention obligation for traffic and localization data with EU law.

Article 126 §1 of the Electronic Communications Act of 13 June 2005 provided that the following providers of publicly available services are subject to data retention obligations:

– landline telephony services;
– mobile telephony services;
– Internet access services;
– Internet email services;
– Internet telephony services;
– providers of underlying public electronic communication networks;
– resellers in their own name and on their own behalf.

---

[151] For further details, see the authors' country report (Belgium) for the Cybercrime Research Centre at Nicolaus Copernicus University (Poland): Paul De Hert and Gertjan Boulet, "The cooperation between Internet service/access providers and law enforcement authorities," February 2015, 29 pp., available at http://www.cybercrime.umk.pl/files/files/Report %20Belgium_De %20Hert %20Boulet.docx

[152] Constitutional Court of Belgium, 11 June 2015, no. 84/2015, available at http://www.const-court.be/public/n/2015/2015-084n.pdf

The Data Retention Act of 29 May 2016 retains these categories in the new version of Article 126, with the exception of resellers in their own name and on their own behalf.

The former version of Article 126 §3 of the Electronic Communications Act of 13 June 2005 established a data retention period of 12 months. The former version of Article 126 §4 of the Electronic Communications Act provided that the King could extend the data retention periods for certain categories of data, without exceeding 18 months, as well as provide a temporary data retention period of more than 12 months. If the data retention period in the latter case exceeded 24 months, then the minister competent for telecommunications could inform the other EU Member States and the European Commission (EC).

The Data Retention Act of 29 May 2016 deletes paragraph 4 of Article 126 and lays down a uniform data retention period of 12 months in Article 126 §3, without the possibility of renewal.

The new version of Article 126 Data Retention Act of the Electronic Communications Act 29 May 2016 retains the requirement that the following data shall be added to the annual reports of the Minister of Justice in implementation of Article 90*decies* CCP:

1° the cases in which data have been provided to the competent authorities in accordance with the applicable legal provisions;

2° the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transfer;

3° the cases in which the data requests could not be met.

A Royal Decree of 19 September 2013 lists the types of data that is subject to data retention.[153]

Article 3 §1 of the Royal Decree of 19 September 2013 provides that landline telephony services retain the following identification data:

1) the number allocated to the user;
2) the user's personal data;
3) the subscription's starting date or the registration data;
4) the type of landline telephony service used and the types of other services with which the user is registered;
5) in case of number transfer, the identity of the transferring provider and of the receiving provider;

---

[153] Royal Decree of 19 September 2013 regarding the execution of Article 126 of the Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 8 October 2013, entry into force on 19 September 2013.

6) the data relating to the payment method, the identification of the payment instrument, and the time of payment for the subscription or for the use of the service.

Article 3 §2 of the Royal Decree of 19 September 2013 provides that landline telephony services retain the following traffic and localization data:

1) the identification of the calling number and the number called;
2) the location of the network connection point of the calling party and of the called party;
3) the identification of all lines in case of group calls, call forwarding, or call transfer;
4) the data and time of the start and end of the call;
5) the description of the telephony service used.

Article 4 §1 of the Royal Decree of 19 September 2013 provides that mobile telephony services retain the following identification data:

1) the number allocated to the user and his International Mobile Subscriber Identity (IMSI);
2) the user's personal data;
3) the date and location of the user's registration or subscription;
4) the date and time of the first activation of the service and the cell ID from which the service is activated;
5) the additional services to which the user has subscribed;
6) in case of number transfer, the identity of the transferring provider;
7) the data relating to the payment method, the identification of the payment instrument, and the time of payment for the subscription or for the use of the service;
8) the ID number of the user's mobile equipment (IMEI).

Article 4 §2 of the Royal Decree of 19 September 2013 provides that mobile telephony services retain the following traffic and localization data:

1) the identification of the telephone number of the calling party and of the called party;
2) the identification of all lines in case of group calls, call forwarding, or call transfer;
3) the IMSI of the calling and called participants;
4) the IMEI of the mobile equipment of the calling and called participants;
5) the data and time of the start and end of the call;
6) the location of the network connection point at the start and the end of each connection;

7) the identification of the geographic location of cells, via reference to the cell ID, at the time of connection;
8) the technical characteristics of the telephony service used.

Article 5 §1 of the Royal Decree of 19 September 2013 provides that Internet access services retain the following identification data:

1) the user ID allocated;
2) the user's personal data;
3) the data and time of the user's registration or subscription;
4) the IP-address, source port of the connection used for subscribing or registering the user;
5) the identification of the network connection point used for subscribing or registering the user;
6) the additional services to which the user has subscribed with the provider concerned;
7) the data relating to the payment method, identification of the payment instrument, and the time of payment of the subscription fee or for the use of the service.

Article 5 §2 of the Royal Decree of 19 September 2013 provides that Internet access services retain the following traffic and localization data:

1) the user's ID;
2a) the IP-address;
2b) in case of shared use of an IP-address, the ports allocated to the IP-address and the data and time of allocation;
3) the identification and location of the network connection point used when logging-in and logging-off;
4) the data and time of an Internet access service session's log-in and log-off;
5) the data volume uploaded and downloaded during a session;
6) the data necessary to identify the geographic location of cells, via reference to the cell ID, at the time of the connection.

Article 6 §1 of the Royal Decree of 19 September 2013 provides that Internet email services and Internet telephony services retain the following identification data:

1) the user ID;
2) the user's personal data;
3) the data and time of creation of the email or Internet telephony account;
4) the IP-address and source port used for the creation of the email or Internet telephony account;

5) the data relating to the payment method, the identification of the payment instrument, and the time of payment of the subscription fee or for the use of the service.

Article 6 §2 of the Royal Decree of 19 September 2013 provides that Internet email services and Internet telephony services retain the following traffic and localization data:

1) the user's ID relating to the email or Internet telephony account, including the number of the ID code of the intended recipient of the communication;
2) the telephony number allocated to each communication entering the telephony network in the context of an Internet telephony service;
3a) the IP-address and the source port used by the user;
3b) the IP-address and the source port used by the addressee;
4) the data and time of the log-in and log-off of a session of the email service or Internet telephony service;
5) the data and time of a connection made by means of the Internet telephony account;
6) the technical characteristics of the service used.

Article 9 §7 of the Electronic Communications Act of 13 June 2005 provides that a specific Royal Decree shall address the matter of data retention for providers of private electronic communications networks and electronic communications services that are not publicly available (closed user groups). Considering the lack of such a Royal Decree, Kerkhofs and Van Linthout argue that Belgian private providers of electronic communications services or networks are currently released from data retention obligations.[154] For the same reason, service providers that act as a mere conduit or provide caching and hosting activities under the Code of Economic Law are currently released from data retention obligations.

As noted (section I.A.2.dd.), legal experts mention the inapplicability of the general data retention legislation for GPS-data and bank accounts. No data retention law seems to govern the collection of GPS-data by Belgian law enforcement requests via car rental companies. However, the National Bank of Belgium, the Belgian Post Group (Bpost), credit institutions, investment companies, insurance companies, banks, notaries, bailiffs, accountants (and others) are subject to specific (less strict) data retention and production obligations of the Act of 18 September 2017 on preventing misuse of the financial system for purposes of laundering money and terrorism financing.

---

[154] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 396.

2. Identification of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

a) Identification of IMEI and IMSI

The Belgian CCP does not have a specific provision for the identification of the device ID (IMEI)[155] and the card number (IMSI).[156] Kerkhofs and Van Linthout explain that the identification of IMEI and IMSI is justified on the basis of Article 46*bis* CCP on the collection of identification data of electronic communications (see section III.C.1.).[157]

b) Location determination via "silent SMS"

In a reply of 9 June 2011 to a parliamentary question regarding the use of "stealth" (silent SMS) technology, the Minister of Justice confirmed that such activities are justified on the basis of Article 88*bis* §1 CCP regarding the tracing of traffic data, and localization of electronic communications.[158]

D. Access to (Temporarily) Stored Communication Data

1. Network search

The network search is embodied in three Articles of the CCP: Articles 39*bis* (non-secret network search during data seizure), Article 89*ter* (network search during looking-in operations) and Article 90*ter* CCP (secret interception and secret network search).

Article 39*bis* §§3-4 CCP, regarding the non-secret network search, read as follows:

> §3. The public prosecutor can extend the search in a computer system or part of it, started on the basis of paragraph 2, to a computer system or a part of it that is in a different location from where the search takes place:
>
> – If this extension is necessary to reveal the truth with regard to the criminal offence that is the object of the search; and

---

155 International Mobile Station Equipment Identity.

156 International Mobile Subscriber Identity.

157 Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 356.

158 Belgian Chamber of Representatives, *Schriftelijke vragen en antwoorden* (Written questions and answers), 2010–2011, no. 53-032, pp. 35–36, available at http://www.dekamer.be/QRVA/pdf/53/53K0032.pdf; see also Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 258.

– If other measures would be disproportionate, or if there is a risk of loss of evidence without this extension.

The extension of the search in a computer system may not extend beyond the computer systems or their parts to which the persons entitled to use the computer system under investigation have access in particular.

With regard to the data found by extending the search in a computer system, which are useful for the same purposes as the seizure, one shall operate as specified in paragraph 6.

If it turns out that these data are not in the territory of the Kingdom, they shall only be copied. In such a case, the public prosecutor shall immediately inform the Federal Public Service Justice, which will inform the competent authority of the State concerned, if the latter can be reasonably determined.

In case of extremely urgent necessity, the public prosecutor can verbally order the extension of the search referred to in the first paragraph. This order shall be confirmed as soon as possible in writing, stating the reasons for the extremely urgent necessity.

§4. Only the investigating judge can order another search in a computer system or part of it than the searches provided for in paragraphs 2 and 3:

– If this search is necessary to reveal the truth with regard to the criminal offence that is the object of the search; and

– If other measures would be disproportionate, or if there is a risk of loss of evidence without this search.

In case of extremely urgent necessity, the investigating judge can verbally order the extension of the search referred to in the first paragraph. This order shall be confirmed as soon as possible in writing, stating the reasons for the extremely urgent necessity.

Article 39*bis* §4 CCP grants exclusive authority to the investigating judge for any searches other than those provided for in paragraphs 2 and 3. As an example of "any other search", the parliamentary preparatory works refer to the example where the authorities seized equipment not connected to a Gmail account.[159] Conings therefore finds that the residual category of searches includes searches directly from government equipment.[160]

Article 89*ter* CCP (network search during looking-in operations) empowers the investigating judge, in the context of the execution of the measure provided for in Article 46*quinquies* CCP (looking-in operations), to gain access to a computer system and to search it. The Act of 25 December 2016 amends Article 89*ter* CCP, by

---

[159] Parliamentary preparatory works, Chamber of Representatives, regarding the improvement of the special investigation methods and certain investigation methods with respect to the internet and electronic and telecommunications, 2015-2016, no. 54 1966/001, p. 21, available at http://www.dekamer.be/FLWB/PDF/54/1966/54K1966001.pdf

[160] Charlotte Conings, *Klassiek en digitaal speuren naar strafrechtelijk bewijs* (The traditional and digital search for criminal evidence), Intersentia, Antwerp/Cambridge, 2017, pp. 136, 298, §§ 195, 475.

providing that the investigating judge has the exclusive authority to order the search of a computer system during looking-in operations.

The parliamentary preparatory works clarify the difference between, on the hand, the network search provided in Article 89*ter* CCP, and, on the other hand, the secret network search provided in Article 90*ter* CCP.[161] The difference lies in the finality of the former, i.e., its exclusive use for two limited cases stated in Article 46*quinquies* §2 CCP in which a looking-in operation may be used:[162]

1) to record the place and to assess the potential presence of goods that are the object of the crime, or that were used to commit the crime, or that result from the crime, or of the presence of profits gained from committing the crime;
2) to collect evidence of the presence of those items.

The parliamentary preparatory works indicate that the network search on the basis of Article 89*ter* CCP can only be used to determine the existence of evidence, and not to collect the evidence; in other words, it is an exploratory instrument that allows at most sampling or copying of part of the evidence. Therefore, the network search in Article 89*ter* CCP allows copying part of a hard drive (e.g., some illegal pornographic images) but not copying the full hard drive.

The legislator's choice to embed the network search in Article 89*ter* CCP instead of Article 46*quinquies* CCP reflects privacy concerns, more specifically a legislative choice to assimilate a computer system with a home (Article 89*ter* CCP) instead of another private place (Article 46*quinquies* CCP). Thus, the legislator has not adopted the approach of Kerkhofs and Van Linthout, who refer to a private "cyber" area as a private place in the meaning of Article 46*quinquies* §1 CCP: they also regard key loggers and spyware as technical means under this Article.[163]

Article 90*ter* CCP embodies the "secret" network search.

Belgian law enforcement agencies do access the cloud on the basis of the network search.[164]

---

[161] Parliamentary preparatory works, Chamber of Representatives, regarding the improvement of the special investigation methods and certain investigation methods with respect to the internet and electronic and telecommunications, 2015-2016, no. 54 1966/001, pp. 51–52, available at http://www.dekamer.be/FLWB/PDF/54/1966/54K1966001.pdf

[162] A looking-in operation on the basis of Article 46*quinquies* CCP is only possible for private places that are not a home or the office of a lawyer of doctor. In case the private place is a home or the office of a lawyer of doctor, then the investigating judge has to authorize the measure (Article 89*ter* CCP).

[163] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, pp. 241, 243.

[164] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, pp. 263, 268 and 295.

2. Search and seizure of stored communications data

a) Special provisions

Article 39*bis*§2, first indent CCP provides an explicit legal basis for a "non-secret" search of a computer system (non-secret information search).

Article 89*ter* CCP provides an explicit legal basis for a network search during looking-in operations.

Article 90*ter* §1, first indent CCP provides an explicit legal basis for a "secret" search of a computer system (secret information search).

Article 39*bis* §2, second indent CCP provides an explicit legal basis for a "data seizure."

b) Applicability of seizure provisions to electronic data

Article 39*bis* §1 CCP provides that the rules on seizure apply to the copying, making inaccessible and deletion of data stored in a computer system or a part of it. Hence, the data seizure (Article 39*bis* CCP) applies to electronic data.

c) Different standards of protection for stored and for transmitted data

As noted (sections III.B.2.b.aa.), the Act of 25 December 2016 embodies the secret network in Article 90*ter* CCP, which nullifies the former legal distinction between interception of "data in transmission" (subject to Article 9*0ter* CCP) and interception of "stored data" (subject to former Article 88*ter* CCP). Hence, the "higher standards"[165] provided in Article 90*ter* CCP apply now to the interception of both data in transmission *and* stored data.

d) Open and clandestine access to stored data

Article 39*bis* §2, first indent CCP provides an explicit legal basis for the "non-secret" search of a computer system (non-secret information search).

Article 90*ter* §1, first indent CCP provides an explicit legal basis for the "secret" search of a computer system (secret information search).

---

[165] As noted (sections II.A.4.a. and III.B.10.c.), the interception measure in Article 90*ter* CCP provides an exception to the general prohibition of the interception of electronic communication provided in Article 314*bis* and Article 259*bis* CC. Article 314*bis* CC lays down the prohibition, applicable to everyone, of taking cognizance of the contents of a telecommunication one does not participate in during the transfer of the telecommunication. A similar prohibition was introduced for public officials in Article 259*bis* CC.

3. Duties to cooperate: production and decryption orders

Article 39*bis* §5 CCP authorizes the public prosecutor or the investigating judge to order the temporary suspension of security or the application of technical means to decipher and decode the data. The investigating judge has exclusive authority to order these measures when this is particularly necessary to extend the search in a computer system (or part of it) to a computer system (or a part of) in a different location. Conings and Oerlemans observe that the use of hacker tools would not be precluded when the investigating judge does not have access to the computer system, and that the use of these tools would not violate the prohibition of hacking provided in Article 550*bis* CC.[166]

Article 39*bis* §6, fourth indent CCP allows the public prosecutor to order the seizure of alleged illegal data (e.g., a computer virus). The public prosecutor can use "all appropriate technical means be used to make inaccessible the data that are the object of the criminal offence or that resulted from the criminal offence and which infringe public order or public decency." This power is used, for example, by prosecutors to request an Internet Service Provider (ISP) to delete from their Domain Name Server (DNS) the domain name of a site that violates the law.

Article 88*quater* CCP (cooperation with individuals and the private sector regarding the network search) allows the public prosecutor to impose on certain individuals the obligation to cooperate during an investigation. These individuals are persons whom the investigating judge thinks have special capacities/knowledge of the computer system that is the object of an investigation or of services used to store, process, encrypt, or transfer data.

Article 90*quater* §2 CCP (secret interception and secret [network] search) obliges operators of an electronic communications network and providers of an electronic communications service to provide cooperation to a secret interception and secret (network) search under Article 90*ter* CCP.

Article 90*quater* §4 (secret interception and secret [network] search) echoes the cooperation referred to in Article 88*quater* CCP, i.e., the power (for the investigating judge, not the public prosecutor) to impose an obligation to cooperate on individuals whom the investigating judge thinks have special capacities/knowledge of the computer system that is the object of an investigation or of services used to store, process, encrypt, or transfer data.

With regard to Article 90*ter* CCP, the fourth functional requirement in Article 6 §1 of the Royal Decree of 9 January 2003 concerns the transfer of content of data

---

[166] Charlotte Conings and Jaap-Jan Oerlemans, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend" (From a network search to an online search: borderless or groundbreaking?), *Computerrecht*, 2013, vol. 5, pp. 23–32, available at https://www.b-ccentre.be/download/b-ccentre_legal/B-CCENTRE %20Van %20een %20 netwerkzoeking%20naar%20online%20doorzoeking.pdf

in plain language if the operator of an electronic communications network or the provider of electronic communications introduced encoding, compression, or encryption of the electronic communications traffic.

All cooperation duties also apply to the suspect, with the exception of the cooperation duty laid down in Article 88*quater* §2 CCP. Kerkhofs and Van Linthout clarify that, whereas Article 88*quater* §2 CCP concerns technical cooperation by the suspect, the other articles concern the provision of mere intelligence or existing evidence.

Kerkhofs and Van Linthout base their argument on an interpretation of the case *Saunders v. the United Kingdom* in which the ECtHR held that:

> [t]he right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused.[167]

However, Kerkhofs and Van Linthout acknowledge that it is still to be seen whether this solution will pass the human rights test by the ECtHR.[168]

Following that logic, it should be asked why the legislator did not excempt the suspect from the cooperation duties referred to in Article 90*quater* §4, which echoes the technical cooperation referred to in Article 88*quater* CCP.

IV. Use of Electronic Communications Data in Judicial Proceedings

1. Use of electronic communications data in the law of criminal procedure

In Belgium, the use of evidence is free. Hence, there are no limits regarding the form by which intercepted material can be introduced as evidence in criminal proceedings.[169]

There are no specific rules on the use of intercepted or stored electronic data as evidence in court proceedings.

---

[167] ECtHR, *Saunders v. the United Kingdom*, Grand Chamber, 17 December 1996, No. 19187/91, §68, available via http://hudoc.echr.coe.int/

[168] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 369.

[169] Raf Verstraeten, *Handboek strafvordering* (Manual on criminal procedure), Antwerp, Maklu, 2007, p. 859; Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, p. 1127.

2. Inadmissibility of evidence as a consequence of inappropriate collection

Illegally obtained evidence follows from:

1) the commission of a criminal offence;
2) a violation of the law of criminal procedure;
3) a violation of the right to privacy;
4) a violation of the right of defence;
5) a violation of the right to human dignity.[170]

However, an illegality committed during evidence collection does not automatically result in the exclusion of the illegally obtained evidence. In its judgment of 14 October 2003, the Supreme Court developed three exclusionary rules, the so-called Antigoon criteria for excluding illegally obtained evidence.[171] More particularly, evidence has to be excluded in three cases:

1) if compliance with procedural rules is legally prescribed under penalty of nullity;
2) if the illegality has compromised the reliability of the evidence;
3) if the use of the illegally obtained evidence violates the right to a fair trial.

In a judgment of 23 March 2004,[172] the Supreme Court held that the violation of the right to a fair trial has to be assessed on the basis of all aspects of the case as a whole, and proposed a number of factors that the judge can take into consideration:

1) whether or not the authorities intentionally committed the illegality;
2) whether the seriousness of the criminal offence exceeds the seriousness of the illegality committed;
3) whether or not the illegality only concerns a material element of the criminal offence;
4) the impact of the illegality on the protected fundamental right;
5) the mere formal nature of the illegality.

The Act of 24 October 2013[173] embodied the Antigoon exclusionary rules in Article 32 of the Preliminary Title of the CCP. However, the Belgian legislator did not incorporate a fourth exclusionary rule developed by the Supreme Court in a judgment of 26 January 2011: an illegality that concerns "a substantial procedural

---

[170] Raf Verstraeten and Frank Verbruggen, *Straf- en strafprocesrecht voor bachelors* (Criminal law and criminal procedural law for bachelors), 11th revised edition, Antwerp-Apeldoorn, Maklu, 2018, p. 323.

[171] Supreme Court, 14 October 2003, P030762N, available via http://jure.juridat.just.fgov.be/

[172] Supreme Court, 23 March 2004, P040012N, available via http://jure.juridat.just.fgov.be/

[173] Act of 24 October 2013 amending the Preliminary Title of the Code of Criminal Procedure, *Belgian Official Journal*, 12 November 2013, entry into force on 22 November 2013.

rule that affects the organization of the courts," i.e., an illegality concerning the material jurisdiction of the courts.[174] The Supreme Court held that this fourth exclusionary rule does not apply if the illegality concerns the territorial jurisdiction of the courts: in this case, exclusion of evidence can only be based on the three traditional Antigoon criteria. In a judgment of 24 April 2013, the Supreme Court effectively applied the fourth exclusionary rule to evidence found during a home search[175] that was authorized by a judge in a police court instead of by the investigating judge.[176]

The investigation methods referred to in this report are not prescribed under sanction of nullity.

Regarding Article 90*quater* §1, 5° CCP, i.e., the duty to mention in the warrant the name and the capacity of the judicial police officer designated for the implementation of the measure, the Supreme Court held in a judgment of 19 June 1967 that an agent other than the one mentioned in the warrant can implement the monitoring measure.[177]

As noted (section III.B.3.a.aa.), although notification to the president of the Bar Association or the representative of the provincial council of the Order of Physicians for an interception measure that covers premises used for business purposes or domicile, or the (tele-)communication means of a lawyer or a doctor (Article 90*octies* §2 CCP), is not prescribed under sanction of nullity, the parliamentary preparatory works underline that the public order nature of this provision implies that failure to do so will entail the nullity of the interception measure.[178]

Apart from the exclusionary rules discussed above, the issue of "admissibility" emerges when a court cannot determine the legality of the evidence.[179] For instance, with regard to a foreign wiretapping measure, the Supreme Court held on 30 March 2010 that the non-availability of sufficient data to assess the legality of one piece of evidence can result in the non-admissibility of that piece; and that the non-availability of sufficient data to assess the legality of all evidence can result in the non-admissibility of the evidence but not in discontinuance of the proceedings.[180]

---

[174] Supreme Court, 26 January 2011, P.10.1321.F, available via http://jure.juridat.just.fgov.be/

[175] On the basis of the Act of 16 November 1972 concerning the Labour Inspectorate, *Belgian Official Journal*, 8 December 1972, entry into force on the same date.

[176] Supreme Court, 24 April 2013, P.12.1919.F.

[177] Supreme Court, 19 June 1967, P.07.0311.

[178] Parliamentary preparatory works, Belgian Senate, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, 1993–1994, 18 May 1994, no. 843-2, p. 189, available at http://www.senate.be/lexdocs/S0539/S05390364.pdf

[179] Raf Verstraeten, *Handboek strafvordering* (Manual on criminal procedure), Antwerp, Maklu, 2012, p. 1015.

[180] Supreme Court, 30 March 2010, P.09.1789.N/1, available via http://jure.juridat.just fgov.be/

On 3 April 2012, the Supreme Court found a violation of the right of defence, as the defence did not have the possibility to assess the legality of evidence resulting from a Dutch wiretapping measure: more specifically, the Court of Appeal of Antwerp had assessed the legality of the evidence merely on the basis of the evidence itself and a letter of the Dutch public prosecutor *(officier van justitie)*.[181] The Supreme Court clarified, however, that the assessment of the legality of the evidence can be based on the authorization of the wiretapping measure.

3. Use of data outside the main proceedings

a) Data from other criminal investigations

The judge does not have a right of injunction against the public prosecutor and thus cannot order the public prosecutor to request the judicial files of other criminal investigations.[182]

Verstraeten and Verbruggen consider that the interception measure should not be discontinued if it reveals information indicating the commission of criminal offences not anticipated by or not mentioned in the interception authorization.[183] These offences are lawfully established only insofar as the execution of the interception measure does not exceed the limits of the authorization. The investigating judge cannot extend the investigation to these offences if no action was brought before him/her in relation to these offences, but must inform the public prosecutor of these offences on the basis of Article 56 §1 *in fine* CCP.

Intercepted data can be used for the prosecution of individuals who were not the subject of the underlying interception order, and if so, only in another criminal investigation.

b) Data from preventive investigations

Data obtained from intelligence services and non-judicial police forces is admissible as evidence in criminal proceedings. Section I.A.4. addressess the legal

---

[181] Supreme Court, 3 April 2012, P.10.0973.N, available via http://jure.juridat.just.fgov.be/

[182] Court of Appeal of Antwerp, 13 March 2002, annotated by Bart De Smet, "Voeging van strafdossiers op verzoek van de verdediging" (Adding a file at the request of the defence), *Rechtskundig Weekblad*, 2002-2003, p. 1022; see Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, p. 615.

[183] Raf Verstraeten and Frank Verbruggen, *Straf- en strafprocesrecht voor bachelors* (Criminal law and criminal procedural law for bachelors), 11th revised edition, Antwerp-Apeldoorn, Maklu, 2018, p. 201, §821.

framework for data exchanges between preventive police authorities/intelligence agencies and law enforcement authorities.

c) Data obtained from foreign jurisdictions

Article 6 of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters provides the general rules on international legal assistance in criminal matters (see below, section V.A.3.).

Article 13 of the Act of 9 December 2004 regarding mutual assistance in criminal matters[184] lays down the rules on the admissibility of intercepted data obtained from foreign jurisdictions. These rules match the Antigoon criteria discussed above (section IV.2.). Article 13 of the Act of 9 December 2004 reads as follows:

> In the context of criminal proceedings conducted before a Belgian court, no use shall be made of evidence:
> 1° which was illegally obtained in a foreign country if the illegality:
> – follows from the infringement of procedural requirements prescribed under sanction of nullity according to the law of the state where the evidence was obtained
> – compromises the reliability of the evidence;
> 2° of which the use would imply a violation of the fundamental right of a fair trial.

4. Challenging the probity of intercepted data

a) Duty to ensure the integrity and confidentiality of the recorded (tele-)communications

Article 90*septies* §1 CCP provides that "[a]ppropriate means shall be used to ensure the integrity and confidentiality of the recorded non-publicly accessible communication or data from a computer system."

In relation to the data seizure measure (Article 39*bis* CCP), Kerkhofs and Van Linthout underlined the need for regulating the chain of custody and for expert reports about the integrity of the evidence.[185] Similar concerns could be raised regarding the integrity and reliability of intercepted data.

b) Access of parties to the judicial file

Article 90*sexies* §4 CCP provides that "[t]he authorizations of the investigating judge, the reports of the judicial police officers referred to in Article 90*quater*, §3,

---

[184] Act of 9 December 2004 regarding mutual assistance in criminal matters and modifying Article 90*ter* of the Code of Criminal Procedure, *Belgian Official Journal*, 24 December 2004, entry into force on 3 January 2005.

[185] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 184.

and the official reports relating to the execution of the measure shall be included in the file at the latest after the termination of the measure."

As noted, the suspect has access to the judicial file on the basis of Article 61*ter* CCP; third parties do not have access to the judicial file (III.B.10.a.).

c) Access of the defence to non-official reports

As noted earlier (see sections III.B.9.a. and b.), Article 90*sexies* §1 CCP lays down reporting requirements regarding the interception measure:

> §1. The designated judicial police officers make available to the investigating judge:
>
> 1° the file containing the recorded non-public communication or data from a computer system obtained as a result of the measures taken in application of the articles 90ter, 90quater and 90quinquies;
>
> 2° the transcription or minutes of the parts of recorded communications or data that the designated police officers deem relevant for the investigation, and any translation thereof;
>
> 3° if applicable, the location of the data referred to in the provision under 2° in the computer system;
>
> 4° a general description of the content and the identification data of the communication means or computer systems used with regard to the communication or data that are not deemed relevant.

According to Article 90*septies* §3 CCP, the files and documents mentioned in Article 90*sexies* §1 CCP do not necessarily need to be recorded in an official record, and as result, not included in the judicial file; if so, then these files and documents qualify as non-official reports.

Nevertheless, all files and documents mentioned in Article 90*sexies* §1 CCP (whether or nor recorded in an official report/judicial file) have to be preserved on the basis of Article 90*septies* §6 CCP:

> The files referred to in Article 90sexies, § 1, 1° shall be kept at the Registry under sealed envelope. Moreover, they can also be kept at the service designated by the King under the conditions and further rules determined by Him after the advice of the Commission for the protection of privacy.
>
> The documents referred to in Article 90sexies, § 1, 2°, 3° and 4°, and the copies of the official reports shall be kept at the Registry under sealed envelope.

Article 90*septies* §6 CCP specifies the access to these files and documents:

> §6. The indicted, the accused, the civil party or their lawyers shall receive, on simple request, a copy of the whole of the recorded non-public communication or data from a computer system, of which certain parts that are deemed relevant for the investigation have been transcribed or minuted and included in an official report that they have access to.
>
> The indicted, the accused, the civil party or their lawyers may request the judge to consult the other files or documents deposited at the Registry in accordance with § 4, and to transcribe or minute additional parts of the recorded communication or data. […]

The judge may reject the request if it does not consider the consultation or transcription or minutes of additional parts necessary to reveal the truth, if it considers it detrimental to the investigation at that time, or for reasons related to the protection of other rights or interests of persons. He can also limit the consultation or transcription or minutes of additional parts to a selection of files or documents he has specified.

d) Right to request additional investigation methods

As noted (section III.B.6.b.), on the basis of Article 61*quinquies* §1 CCP, the suspect and the civil party have the right to request that the investigating judge carry out additional investigation methods, such as the appointment of an expert or performance of a second test.[186]

According to Article 61*quinquies* §2 CCP, the suspect and the civil party shall submit their petition for an additional investigation method in writing to the Registry of the Court of First Instance. The petition should be substantiated and give a detailed description of the requested investigation method.

According to Article 61*quinquies* §3 CCP, the judge may reject the request if he considers the measures to be unnecessary in order to reveal the truth or if, at that moment, he considers the measures prejudicial to the investigation. According to Article 61*quinquies* §4 CCP, rejection by the investigating judge is subject to appeal before the Indictment Chamber (see section I.A.4.b.), in which case the investigating judge shall hear the Prosecutor General, the suspect, and his or her attorney (Article 61*quater* §5 CCP).

Even though there is no explicit legal basis for this, the trial judge can also order the appointment of an expert or a second test at his own request. This power is intrinsic to the judge's general mandate of the finding of truth.

e) Non-disclosure of technical means

In a reply of 9 June 2011 to a parliamentary question (see section III.C.2.b.), the Minister of Justice explained that the use of "stealth" technology is allowed under Article 88*bis* CCP (tracing of traffic data, and localization of electronic communications). However, at the same time, the Minister of Justice recalled that the prohibition of disclosure of the technical means used for special investigation methods, such as the observation and the infiltration (Article 47*sexies* CCP), also applies to Article 88*bis* CCP.[187] Hence, it could be asked to what extent the same rationale

---

[186] Cf. Philip Traest, "Judicial control on the gathering and reliability of technical evidence in a continental criminal justice system," conference paper for the 16th International Conference of the International Society for the Reform of Criminal Law, 2002, p. 10, available at http://www.isrcl.org/Papers/Traest.pdf

[187] Belgian Chamber of Representatives, *Schriftelijke vragen en antwoorden* (written question and answers), 2010-2011, no. 53-032, p. 36, available at http://www.dekamer.be/QRVA/pdf/53/53K0032.pdf; see also Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 258.

holds for the powers of looking-in operations (Articles 46*quinquies* and 89*ter* CCP), the cyber infiltration (Article 46*sexies* CCP) and the interception measure (Article 90*ter* CCP).

f) Exclusion of unreliable evidence

The second Antigoon criterion demands exclusion of illegally obtained evidence if the illegality has compromised the reliability of the evidence (see section IV.2.).

V. Exchange of Intercepted Electronic Communications Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

1. International conventions

a) UN conventions

United Nations Convention against Transnational Organized Crime of 15 November 2000:[188] signature on 12 December 2000, ratification on 11 August 2004.[189] According to Article 38 §1 of the Convention (on the entry into force of the Convention), "[t]his Convention shall enter into force on the ninetieth day after the date of deposit of the fortieth instrument of ratification, acceptance, approval or accession." Hence, the Convention entered into force on 9 November 2001.

Belgium made no declarations, reservations, or notifications specifically regarding the interception of electronic communication.[190]

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20 December 1988:[191] signature on 22 May 1989, ratification on 25 October 1995. According to Article 29 §2 of the Convention (on the entry

---

[188] United Nations Convention against Transnational Organized Crime, General Assembly Resolution 55/25 of 15 November 2000, the conventions and the protocols thereto are available at http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC %20 Convention/TOCebook-e.pdf

[189] Act of 24 June 2004 regarding the approval of the Convention against Transnational Organized Crime and its protocols, *Belgian Official Journal*, 13 October 2004, entry into force on 23 October 2004.

[190] The declarations and notifications by Belgium at the time of depositing (11 August 2004) the instrument of ratification of the United Nations Convention against Transnational Organized Crime are available here https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&lang=en#EndDec

[191] United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Vienna, 20 December 1988. The convention is available via https://treaties.un.org/

into force of the Convention), "[f]or each State […] ratifying, accepting, approving or acceding to this Convention after the deposit of the twentieth instrument of ratification, acceptance, approval or accession, the Convention shall enter into force on the ninetieth day after the date of the deposit of its instrument of ratification, acceptance, approval or accession." Hence, the Convention entered into force in Belgium on 23 January 1996. Belgium made no declarations, reservations, or notifications specifically regarding the interception of electronic communication.

b) Council of Europe conventions

European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 (CETS No. 030):[192] signature on 20 April 1959, ratification on 13 August 1975.[193] Article 27 §3 of the Convention (under chapter VIII on final provisions) provides: "As regards any signatory ratifying subsequently the Convention shall come into force 90 days after the date of the deposit of its instrument of ratification." Hence, the Convention entered into force in Belgium on 11 November 1975.

Of note are the following reservations made by Belgium, at the time of depositing the instrument of ratification with the Secretary General of the Council of Europe. These reservations cover the period since the entry into force of the Convention on 11 November 1975:

Concerning Article 2 of the Convention (on the refusal of assistance, under chapter I on general provisions):[194]

> The Government of the Kingdom of Belgium reserves the right not to comply with a request for assistance
>
> a. if there are good grounds for believing that it concerns an inquiry instituted with a view to prosecuting, punishing or otherwise interfering with an accused person because of his political convictions or religion, his nationality, his race or the population group to which he belongs;
>
> b. is so far as it concerns a prosecution or proceedings incompatible with the principle non bis in idem;
>
> c. in so far as it concerns an inquiry into acts for which the accused person is being prosecuted in Belgium.

Concerning Article 22 of the Convention (single article under chapter VII. on the exchange of information from judicial records):

---

[192] European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 20 April 1959, available at http://conventions.coe.int/treaty/en/Treaties/Html/030.htm

[193] Act of 19 July 1975 regarding approval of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, *Belgian Official Journal*, 23 October 1975, entry into force on 11 November 1975.

[194] The reservations and declarations made by Belgium at the time of depositing (13 August 1975) the instrument of ratification of the Convention on Mutual Assistance in Criminal Matters of 20 April 1959 are available via https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/030

> The Government of the Kingdom of Belgium will not notify the subsequent measures referred to in Article 22 except in so far as the organisation of its judicial records allows of so doing.

Concerning Article 26 of the Convention (relation of the Convention to other legal instruments, under chapter VIII on final provisions):

> By reason of the special arrangements between the Benelux countries, the Government of the Kingdom of Belgium does not accept Article 26, paragraphs 1 and 3 in respect of its relations with the Netherlands and Luxembourg.
>
> The Government of the Kingdom of Belgium reserves the right to derogate from these provisions in respect of its relations with other member States of the European Economic Community.

Belgium also signed the two additional protocols to the *European Convention on Mutual Assistance in Criminal Matters:*

The *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, 17 March 1978:[195] signature on 11 July 1978, ratification on 28 February 2002.[196] The additional protocol entered into force in Belgium on 29 May 2002.

The *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, 8 November 2001:[197] signature on 8 November 2011, ratification on 9 March 2009.[198] The additional protocol entered into force in Belgium on 1 July 2009.

Convention on Cybercrime (CETS No. 185):[199] signature on 23 November 2001, ratification on 20 August 2012.[200] According to Article 36 §4 of the Convention:

> the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention.

Hence, the Convention entered into force in Belgium on 1 December 2012.

---

[195] Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 17 March 1978, available at http://conventions.coe.int/treaty/en/Treaties/Html/099.htm

[196] Act of 29 January 2002 regarding approval of the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, *Belgian Official Journal*, 1 June 2002, entry into force on 11 June 2002.

[197] Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 8 November 2001, available at http://conventions.coe.int/treaty/en/Treaties/Html/182.htm

[198] Act of 8 November 2001 regarding approval of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, *Belgian Official Journal*, 19 June 2009, entry into force on 1 July 2009.

[199] Cybercrime Convention, Budapest, 23 November 2001, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[200] Act of 3 August 2012 regarding approval of the Cybercrime Convention, *Belgian Official Journal*, 21 November 2012, entry into force on 1 December 2012.

Belgium made no reservations or declarations specifically regarding the interception of electronic communication.[201]

As noted (see section III.A.1.), Article 39*ter* CCP (preservation request for natural persons or legal persons) embodies the implementation of Articles 16 and 17 of the Cybercrime Convention; and Article 39*quater* CCP (preservation request for foreign authorities) embodies the implementation of Articles 29 and 30 of the Cybercrime Convention.

c) EU conventions

Treaty between the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands concerning extradition and mutual assistance in criminal matters (Benelux Treaty), 27 June 1962:[202] signature on 27 June 1962, ratification on 30 July 1964.[203] Article 49 §2 of the Convention provides that "[t]he Treaty shall enter into force two months after the deposit of the last instrument of ratification." Hence, the treaty entered into force on the same date for Belgium, Luxembourg, and the Netherlands. The Netherlands deposited the last instrument of ratification on 11 October 1967. Hence, the treaty entered into force two months later, on 11 December 1967.

Belgium made no declarations specifically regarding the interception of electronic communication.[204]

Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 29 May 2000:[205] signature on 29 May 2000, ratification on 25 May 2005.[206] Article 27 §§2–3 of the Convention read as follows:

---

[201] The declaration of Belgium at the time of depositing (20 August 2012) the instrument of ratification of the Cybercrime Convention is available at http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=&DF=&CL=ENG&VL=1

[202] Treaty between the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands concerning extradition and mutual assistance in criminal matters, Brussels, 27 June 1962, available via https://verdragenbank.overheid.nl/en/Treaty/Details/009118.html

[203] Act of 27 June 1962 regarding the approval of the Treaty between the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands concerning extradition and mutual assistance in criminal matters, *Belgian Official Journal*, 24 October 1967, entry into force on 11 December 1967.

[204] The declarations of Belgium under the Benelux Treaty are available at the end of the Treaty.

[205] Council Act of 29 May 2000 establishing, in accordance with Article 34 of the Treaty on European Union, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, pp. 1–23.

[206] Act of 11 May 2005 regarding approval of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *Belgian Official Journal*, 22 June 2006, entry into force on 2 July 2005.

> 2. Member States shall notify the Secretary-General of the Council of the European Union of the completion of the constitutional procedures for the adoption of this Convention. 3. This Convention shall, 90 days after the notification referred to in paragraph 2 by the State, member of the European Union at the time of adoption by the Council of the Act establishing this Convention, which is the eighth to complete this formality, enter into force for the eight Member States concerned.

Hence, the Convention entered into force in Belgium on 23 August 2005.

Belgium made no declarations specifically regarding the interception of electronic communication.[207]

Belgium also signed the additional protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union:

– *Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*, 16 October 2001:[208] signature on 16 October 2001, ratification on 25 May 2005.[209] The additional protocol entered into force in Belgium on 5 October 2005.

– *Convention on Mutual Assistance in Criminal Matters between the European Union and the United States of America, 25 June 2003*.[210]

– *European Investigation Order,* 3 April 2014 (see section V.C.).[211] Belgium transposed the European Investigation Order by the Act of 22 May 2017.[212]

2. Bilateral treaties

Article 25 §2 of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 provides that "[t]he Contracting Parties may conclude between themselves bilateral or multilateral agreements on mutual assistance in

---

[207] The declaration of Belgium of 23 March 2011 under the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union is available at https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties.aspx?Id=18

[208] Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 326, 21.11.2001, pp. 2–8.

[209] Act of 11 May 2005 regarding approval of the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *Belgian Official Journal*, 22.6.2005, entry into force on 2 July 2005.

[210] Approved by the Act of 30 June 2009 (*Belgian Official Journal*, 8 March 2010, entry into force on 18 March 2010).

[211] The European Parliament and the Council of the European Union, Directive 2014/41/EU of the European Parliament and of the Council of the European Union of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, pp. 1–36.

[212] Act of 22 May 2017, Act regarding the European Investigation Order, *Belgian Official Journal*, 23 May 2017, entry into force on 22 May 2017.

criminal matters only in order to supplement the provisions of this Convention or to facilitate the application of the principles contained therein."

Accordingly, via letters signed on 6 March and 18 July 1975, Belgium and Germany concluded an additional bilateral agreement for cases in which the request for assistance concerns the following:

1) a civilly liable person who is involved in a criminal case, or
2) criminal investigations in fiscal matters (customs and excise, direct or indirect taxation, and exchange control).[213]

These cases were already provided in the provisions 2a-b of the additional protocol to the extradition and mutual legal assistance treaty between Belgium and Germany of 17 January 1958.[214]

The bilateral agreement with Germany does not include any specific provisions regarding the interception of electronic communication. Neither do the other mutual legal assistance treaties (MLATs) with Belgium:

– Agreement between the People's Republic of China and the Kingdom of Belgium on mutual legal assistance in criminal matters, 31 March 2014.[215]

– Agreement between Brazil and Belgium on mutual legal assistance in criminal matters, 7 May 2009.[216]

– Agreement on mutual legal assistance in criminal matters between the Kingdom of Belgium and the Republic of Korea, 17 January 2007.[217]

– Agreement between the Government of the Kingdom of Belgium and the Government of the Kingdom of Thailand on mutual legal assistance in criminal matters, 12 November 2005.[218]

---

[213] See Point 1.A of the agreement. An extract of the agreement is available on the website of the online legal database Vlex: http://vlex.be/vid/wisseling-brieven-belgi-bonds republiek-strafbare-30519154

[214] See the doctoral thesis of Professor Gert Vermeulen, *Wederzijdse rechtshulp in strafzaken in de Europese Unie* (mutual legal assistance in criminal matters in the European Union), Antwerp-Apeldoorn, Maklu, 1999, pp. 70–71, footnote 266; see also Gert Vermeulen, Tom Vander Beken, Els De Busser, Chris Van den Wyngaert, Guy Stessens, Adrien Masset, and Christophe Meunier, *Een nieuwe Belgisch wetgeving inzake internationale rechtshulp in strafzaken* (New Belgian legislation regarding international legal assistance in criminal matters), Antwerp-Apeldoorn, Maklu, 2002, p. 122, footnote 87.

[215] Approved by the Act of 13 March 2016 (*Belgian Official Journal*, 26 April 2016, entry into force on 22 April 2016).

[216] Approved by the Act of 5 May 2014 (*Belgian Official Journal*, 2 May 2017, entry into force on 12 May 2017).

[217] Approved by the Act of 10 July 2012 (*Belgian Official Journal*, 2 October 2012, entry into force on 29 September 2012).

[218] Approved by the Act of 19 June 2008 (*Belgian Official Journal*, 13 July 2010, entry into force on 23 July 2010).

– Agreement Between the Government of the Hong Kong Special Administrative Region of the People's Republic of China and the Government of the Kingdom of Belgium Concerning Mutual Legal Assistance in Criminal Matters, 20 September 2004.[219]

– Agreement between the Kingdom of Belgium and the United States of America on mutual legal assistance in criminal matters, 28 January 1998.[220]

– Agreement between the Kingdom of Belgium and the Kingdom of Morocco on mutual legal assistance in criminal matters, 7 July 1997.[221]

– Treaty between the Government of Canada and the Government of the Kingdom of Belgium on Mutual Legal Assistance in Criminal Matters, 11 January 1996.[222]

3. National regulation

Article 6 of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters provides the general rules on international legal assistance in criminal matters (see section IV.3.c.):[223]

> §1. Requests for mutual legal assistance in criminal matters by the competent foreign authorities shall be implemented in accordance with Belgian law and, where appropriate, in accordance with the applicable international legal instruments binding on the requesting State and Belgium.
>
> §2. However, if the request for mutual legal assistance so provides and an international instrument binding on Belgium and the requesting State provides for such an obligation, this request shall be implemented in accordance with the procedural rules expressly referred to by the foreign authorities, provided that those rules do not limit fundamental rights and do not detract from any other fundamental principle of Belgian law.
>
> §3. A request for mutual legal assistance in criminal matters can also, within the limits provided for in §2, be implemented in accordance with the procedural rules explicitly mentioned by the foreign authorities in the absence of an international instrument binding Belgium and the requesting State and that provides for such an obligation.
>
> §4. In the event that a request for mutual legal assistance in criminal matters cannot be implemented for legal reasons, the Belgian authorities responsible for this shall immediately notify the competent foreign authorities of this by a reasoned decision and, if applicable, state the conditions under which this execution could still take place.

---

[219] Signed on 20 September 2004; approved by the Act of 5 August 2006 (*Belgian Official Journal*, 11 December 2006; entry into force on 1 December 2006).

[220] Signed on 28 January 1998; approved by 4 March 1998 (*Belgian Official Journal*, 8 December 1998, entry into force on 18 December 1999.

[221] Signed on 7 July 1997; approved by the Act of 24 February 2005 (*Belgian Official Journal*, 29 April 2005, entry into force on 1 May 2005).

[222] Signed on 11 January 1996; approved by the Act of 9 January 2003 (*Belgian Official Journal,* 19 March 2003, entry into force on 1 April 2003).

[223] Act of 9 December 2004 regarding mutual assistance in criminal matters and modifying Article 90ter of the Code of Criminal Procedure, *Belgian Official Journal*, 24 December 2004, entry into force on 3 January 2005.

> In the event that a request for mutual legal assistance in criminal matters cannot be implemented within the deadlines set, the Belgian authorities responsible for this shall immediately notify the competent foreign authorities, clearly describing the reasons for the delay and the period within which the implementation can take place.
>
> §5. If, following the implementation of a request for mutual legal assistance, goods were seized that are object of the crime according to the request for mutual legal assistance, a third party concerned may object to the transferring of these seized goods to the requesting authority.
>
> […]

Hence, Article 6 §4 of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters enables non-treaty-based assistance for the interception of electronic communication.

B. Requirements and Procedure (Including the Handling of Privileged Information)

1. Incoming requests

a) Designation of authorities on the basis of Belgian law: no consent needed from the Belgian Minister of Justice for requests from EU Member States

Article 5 §1 of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters provides that the consent of the Minister of Justice is not required for the implementation in Belgium of requests for mutual assistance from EU Member States.

However, Article 5 §2 of the Act of 9 December 2004 provides that the consent of the Minister of Justice is required when the request can be refused on the basis of one of the three reasons provided in Article 4 §1 of the same Act:

1) to reduce the risk that the death penalty will be imposed;
2) in case the suspect requests refusal of the mutual legal assistance request;
3) in case the requesting state does not give sufficient guarantees that the death penalty will not be pronounced or executed.

In these cases, Article 5 §2 of the Act provides that the Belgian judicial authorities, or the Prosecutor General if the public prosecutor and the investigating judge receive the request, shall send the foreign request to the Minister of Justice.

An *a contrario* reading of Article 5 §1 of the Act of 9 December 2004 implies that the consent of the Minister of Justice is required for the implementation in Belgium of requests for mutual assistance from non-EU Member States.

Article 7 §1, 2° of the Act prescribes that requests for mutual assistance from foreign authorities shall be addressed to the Belgian judicial authorities via diplo-

matic channels. Belgium shall send the records relating to the implementation of the measure to the requesting state in the same way.

b) Designation of authorities on the basis of international instruments

Article 7 §2 of the Act of 9 December 2004 provides that an international instrument may prescribe that mutual legal assistance takes place either between the foreign authority and the Belgian judicial authorities or between the Ministries of Justice of the requesting state and Belgium.

However, Article 7 §4 of the Act of 9 December 2004 provides that, if the foreign request concerns a case that can seriously harm the public order or essential interests of Belgium, the federal prosecutor, or the Prosecutor General if the public prosecutor and the investigating judge receive the request, shall immediately send an information report to the Minister of Justice.

Two of the international instruments regarding mutual legal assistance determine the competent authorities for implementing mutual legal assistance requests:

– the *European Convention on Mutual Assistance in Criminal Matters of 20 April 1959* (Article 15);

– the *Treaty between the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands concerning extradition and mutual assistance in criminal matters (Benelux Treaty) of 27 June 1962* (Article 30).

The other international instruments allow the parties to designate the relevant authorities.

Belgium designated the Directorate-General legislation, fundamental rights and freedoms[224] of the Federal Public Service Justice as the competent authority under Article 18(13) of the United Nations Convention against Transnational Organized Crime of 15 November 2000 and under Article 24 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[225]

Belgium designated the International Criminal Cooperation Department[226] of the Federal Public Service Justice as the competent authority under Article 24.7.a (making or receiving requests for extradition or provisional arrest) and Article 27.2

---

[224] *Directoraat-generaal Wetgeving en Fundamentele Rechten en Vrijheden* (DG WL, in Dutch), *Direction générale de la Législation et des Libertés et Droits fondamentaux* (DG WL, in French).

[225] See the declaration of Belgium of 23 March 2011 under the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, available at https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties.aspx?Id=18

[226] *Dienst Internationale Samenwerking in Strafzaken* (in Dutch), *Service de la coopération internationale pénale* (in French).

(sending and answering requests for mutual assistance) of the Cybercrime Convention.[227]

Belgium designated the Federal Computer Crime Unit (FCCU) of the Federal Judicial Police (Directorate for Combating Economic and Financial Crime) as the competent authority under Article 35 (24/7 point of contact) of the Cybercrime Convention.

Belgium designated the Public Prosecutor's Office and the General Administration Customs and Excise as the competent requested authorities under the European Investigation Order.

c) Reporting duties to the Ministry of Justice

Article 7 §3 of the Act of 9 December 2004 provides that the Belgian judicial authorities shall send a copy of every received request for mutual assistance to the Federal Public Service Justice.[228]

d) No filtering duties and no destruction duties

Belgian law does not subject the Belgian authorities to a duty to filter out or delete privileged information before transmitting the results of an interception measure to a foreign country (see section B.3.). As noted earlier in this section, in special cases, the Minister of Justice will decide whether or not to respond to a foreign mutual legal assistance request.

Belgian law does not prohibit retention of data that has been intercepted following a request for mutual legal assistance.

e) No rules for protecting the individual: no notification obligations and remedies

According to legal experts, there are no specific rules for protecting individuals in case of cross-border interception and MLA.

---

[227] See the declaration of Belgium at the time of depositing (20 August 2012) the instrument of ratification of the Cybercrime Convention, available at http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=&DF=&CL=ENG&VL=1

[228] *Federale Overheidsdienst Justitie* (in Dutch), *Service Public Fédéral Justice* (in French); see the notification by Belgium at the time of depositing (11 August 2004) the instrument of ratification of the United Nations Convention against Transnational Organized Crime, available at https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&lang=en#EndDec

f) No data destruction obligations

According to legal experts, Belgian authorities can store data that has been intercepted and transferred (immediately or subsequently) to the requesting State. Furthermore, Belgian authorities have no obligation to destroy the data.

2. Outgoing requests

a) Designation of authorities on the basis of Belgian law: consent needed from the Belgian Minister of Justice for requests from Belgium

The principle of no consent by the Minister of Justice for requests from EU Member States, set forth in Article 5 §1 of the Belgian Act of 9 December 2004 concerning international mutual legal assistance in criminal matters, does not apply to mutual assistance requests from Belgian to EU Member States. Article 7 §1 1° of the Act provides that the Belgian judicial authorities shall use diplomatic channels, via the Minister of Justice, to send the mutual assistance request as well as the records relating to the implementation of the measure to the foreign state.

b) Designation of authorities on the basis of international instruments

Article 7 §2 of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters (regarding the designation of authorities by international instruments), as well as the exceptions thereto provided in Article 7 §4 of the same Act, also apply to cases of foreign requests for mutual assistance to Belgium (see section V.B.1.b.).

Belgium designed the Public Prosecutor's Office, the investigating judge and the General Administration Customs and Excise as the competent requesting authorities under the European Investigation Order (see section V.C.).

c) Exclusion of foreign evidence

See section IV.3.c.

3. Real-time transfer of communications data

Article 14 2° of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters inserts §§6–7 into Article 90*ter* CCP (see also section III.B.9.b.), which implement Article 20 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (see

section V.A.1.).[229] Article 20 of the Convention refers to the interception of electronic communications without the technical assistance of another Member State and addresses situations in which the suspect either is situated in border areas where the networks of Belgian and foreign operators intertwine or uses satellite communication. In these cases, the requesting state can intercept the communications as long as the requested state has not given a negative answer.

Article 90*ter* CCP §§6–7 read as follows:

> §6. A competent foreign authority can, in the context of a criminal investigation, temporarily intercept, take cognizance of and record non-public communication or data of a computer system, if the person to whom this measure relates is located on the Belgian territory and if the following conditions are met:
>
> 1° this measure does not require technical intervention by a body established in Belgium;
>
> 2° the foreign government involved has notified this measure to a Belgian judicial authority;
>
> 3° this possibility is provided in an international legal instrument between Belgium and the requesting State;
>
> 4° the decision of the investigating judge referred to in § 7 has not yet been communicated to the foreign government concerned.
>
> The data gathered on the basis of this paragraph can only be used on condition that the competent Belgian authority has agreed with the measure.
>
> §7. Once the public prosecutor receives the notice referred to in paragraph 6, first section, 2° he shall immediately bring the notice before the investigating judge.
>
> The investigating judge before whom a notice referred to in § 6, first section, 2° is brought approves the measure if it is permissible in accordance with the provisions of this article.
>
> He shall inform the foreign government concerned of his decision within ninety-six hours from receipt by the Belgian judicial authorities.
>
> In case an additional period is necessary, the investigating judge can postpone his decision and its notice to the competent foreign authorities for a maximum of eight days. He shall immediately notify the competent foreign authority of this, stating the reasons.
>
> In case the investigating judge does not allow the measure referred to in § 6, he shall also notify the foreign government that the gathered data must be destroyed and cannot be used.

Legal experts have explained that, in practice, foreign authorities will be present during real-time interception of electronic communications by Belgian authorities.

---

[229] Parliamentary preparatory works, Chamber of Representatives, regarding international mutual assistance in criminal matters, 2003–2003, no. 51 1278/001, pp. 21–22, available at http://www.dekamer.be/FLWB/pdf/51/1278/51K1278001.pdf

C. European Investigation Order

Belgium transposed the European Investigation Order (EIO) by the Act of 22 May 2017, which includes specific provisions on the cross-border interception of electronic communications (Articles 38 and 39).

Article 38 of the Act of 22 May 2017 almost literally transposes Article 30 of the EIO (interception of telecommunications with technical assistance of another Member State). The only addition by Article 38 is the implementation of Article 30 §5, second indent of the EIO, which allows the executing State to make its consent subject to any conditions which would be observed in a similar domestic case.

For an EIO aimed at "transmitting telecommunications immediately to the issuing State" (Article 30 §6 (a) EIO), Article 38 §8, second indent of the Act of 22 May 2017 subjects Belgium's consent as executing state to only some (not all) conditions that would have to be observed in a similar domestic case:

– the period during which the measure can be carried out shall not be longer than one month (Article 90*quinquies* §1, 4° CCP);

– in derogation of Article 90*quater* §3, third indent CCP, the designated judicial police officers do not have to report in writing to the investigating judge about the execution of the authorization every five days;

– the investigating judge can prolong the operation of the authorization referred to in Article 90*quater* § 1 CCP one or more times with a term that may not be longer than one month, with a maximum of six months, without prejudice to his decision to terminate the measure as soon as the circumstances that justified the measure have disappeared (Article 90*quinquies*, first indent CCP);

– the investigating judge shall request the issuing State to provide precise circumstances that warrant the prolongation of the measure (Article 90*quinquies*, second indent CCP). In addition to what is foreseen in Article 90*quinquies*, second indent CCP, the investigating judge shall also request the issuing State to provide "any useful information" that warrants the prolongation of the measure. In order to facilitate the necessity of mentioning in the authorization the precise circumstances that warrant the prolongation of the measure, the issuing State shall provide these precise circumstances and any useful information "at the latest seven days before the end of the period of one month."

For an EIO aimed at "intercepting, recording and subsequently transmitting the outcome of interception of telecommunications to the issuing State" (Article 30 §6 (b) EIO), Article 38 §8, third indent of the Act of 22 May 2017 subjects Belgium's consent as executing state to all conditions that would have to be observed in a similar domestic case (Articles 90*ter* to 90*novies* CCP; see the relevant sections in this report).

Article 39 literally transposes Article 31 of the EIO (notification of the Member State where the subject of the interception is located from which no technical assistance is needed).[230]

According to legal experts, both the EIO and the European Arrest Warrant[231] have the advantages of approximating procedural criminal law, administrative simplification and more efficient (faster) cooperation. However, they also observed that both instruments have reduced the efficiency of certain MLA requests. For example, in the Belgian report for INTLI 1,[232] we wrote that the EIO order will increase cases in which foreign procedural law applies to evidence gathering on Belgian territory: Article 9.2 EIO (literally transposed in Article 19.2 of the Belgian Act of 22 May 2017) provides that "[t]he executing authority shall comply with the formalities and procedures expressly indicated by the issuing authority unless otherwise provided in this Directive and provided that such formalities and procedures are not contrary to the fundamental principles of law of the executing State."[233] In practice, this means that Belgium as executing State may need to respect the issuing State's definitions regarding procedural powers. For example, the legal experts said that, before the adoption of the EIO, Belgian public prosecutors were allowed to execute an MLA request for a computer search. However, with the EIO's focus on the procedural law of the issuing State, Belgian authorities have to respect the issuing State's potential classification of the Belgian computer search as a network search rather than a computer search. Hence, considering that the competence for executing a network search on the basis of Article 90*ter* CCP lies with the investigating judge, the public prosecutor is then obliged to immediately transfer an EIO/request for a secret network search to the investigating judge, who has to control the request before authorizing its execution by the public prosecutor.[234]

---

230 Compare with Articles 39*bis* CCP (non-secret network search during data seizure), and 90*quater* CCP (secret interception and secret (network) search): although both articles enshrine the former Article 88*ter* CCP notification duty towards States in case of a cross-border access network search, legal experts observed that, as of 2001, the legal obligation to notify foreign authorities of a network search on their territory has never been respected.

231 Council of the European Union, Council Framework Decision of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member States, 2002/584/JHA, OJ L 190, 18.7.2002, pp. 1–20.

232 See INTLI 1, Belgian report, p. 240.

233 See also section V.A.3.: Article 6 §2 of the Belgian Act of 9 December 2004 concerning international mutual legal assistance in criminal matters allows the implementation of foreign mutual assistance requests in accordance with foreign procedural law "if provided in the request for mutual legal assistance and if an international instrument that binds Belgium and the requesting State provides for such an obligation […], provided that those rules do not restrict fundamental rights and without prejudice to any other principle of Belgian law."

234 Article 16 of the Act of 22 May 2017 explicitly empowers the investigating judge for the execution of investigation methods that in a similar national procedure have to authorized by an investigating judge.

Furthermore, legal experts underlined the remaining problem of double incrimination. For example, the definition of hacking under Belgian law (Article 550*bis* CC) is broad, including unauthorized wifi-connections (unlike under German law).

D. Statistics

Our attempts to obtain data from the Ministry of Justice regarding the extent of MLA-requests for electronic communications interception were unsuccesful.

According to legal experts, the MLAT procedure is slow and inefficient. However, they stated that the MLAT procedure works well among MLAT experts, such as within the European Judicial Cybercrime Network (EJCN), which is supported by the EU agency Eurojust.[235]

Legal experts have noted that, in most cases, MLA demands relate to the content of emails. And they have also noted the relevance of informal cooperation among judicial authorities, beyond the scope of MLA.

Bibliography*

Arnou, Luc, "Afluisteren tijdens het gerechtelijk onderzoek" (Wiretapping during the investigation); in Commentaar Strafrecht en strafvordering (Commentary criminal law and criminal procedural law), Gent, Kluwer, 2008, vol. 59, 95 pp.

Belgian Chamber of Representatives, *Schriftelijke vragen en antwoorden* (written questions and answers), 2010-2011, no. 53-032, 79 pp., available at http://www.dekamer.be/QRVA/pdf/53/53K0032.pdf

Belgian Institute for Postal Services and Telecommunications, "Synthese van de raadpleging door de raad van het bipt op verzoek van de minister voor ondernemen en vereenvoudigen van 29/04/2010 betreffende de praktische uitvoering van richtlijn 2006/24/EG van 15 maart 2006 (richtlijn betreffende de bewaring van gegevens)" (Summary regarding the implementation of the data retention directive 2006/24/EG of 15 March 2006), 2010, p. 14, available at http://www.bipt.be/public/files/nl/12593344_nl_2010-10-01_bipt-verslag_consultatie_data_retention-publieke_versie_v20101001_nl.pdf

---

235 The European Judicial Cybercrime Network (EJCN) "was established in 2016, during the Dutch EU Presidency, to foster contacts between practitioners specialised in countering the challenges posed by cybercrime, cyber-enabled crime and investigations in cyberspace, and to increase efficiency of investigations and prosecutions." For more information on ECJN, see http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx

* All URLs were last accessed in 2/2020.

Belgian Standing Intelligence Agencies Review Committee (Standing Committee I), "Activity reports", available (in Dutch and French) at http://www.comiteri.be/

Board of Prosecutors General, "Telecommunicatierichtlijn inzake het opsporings- en vervolgingsbeleid betreffende inbreuken op de medewerkingsverplichtingen vervat in de artikelen 46bis §2, 88bis §2 en 90quater §2 van het wetboek van strafvordering" (Telecommunications Circular regarding the investigation and prosecution of violations of the cooperation duties under Articles 46*bis* §2, 88*bis* §2 and 90*quater* §2 CCP), COL 14/2009, 17 December 2009, 11 pp., available (in Dutch and French) at https://www.om-mp.be/

Board of Prosecutors General, Circular of 15 June 2005 regarding the Autonomic Police Treatment and the simplified official records, COL 8, available (in Dutch and French) at https://www.om-mp.be/

Bockstaele, Marc and others (eds.), *De Zoeking onderzocht* (An analysis of the search), Antwerp-Apeldoorn, Maklu, 2009, 403 pp.

Boulet, Gertjan, "Regulating Surveillance: The Belgian case," Deliverable 2.3 (The Legal Perspective) for the EU-funded project Increasing Resilience in Surveillance Studies (IRISS), pp. 49–52, 31 January 2013, available at http://irissproject.eu/wp-content/uploads/2013/04/Legal-perspectives-of-surveillance-and-democracy-report-D2.3-IRISS.pdf

Bourlet, Christina, "La lutte contre la fraude de mass: développements récents" (The fight against mass fraud: recent developments); in Dominique Grisay (ed.), *De la lutte contre la fraude à l'argent du crime: État des lieux,* Brussels, Groupe De Boeck, 2013, pp. 83–98.

Conings, Charlotte, *Klassiek en digitaal speuren naar strafrechtelijk bewijs* (The traditional and digital search for criminal evidence), Intersentia, Antwerp/Cambridge, 2017, 862 pp.

Conings, Charlotte and Oerlemans, Jaap-Jan, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend" (From a network search to an online search: borderless or groundbreaking?), *Computerrecht*, 2013, vol. 5, pp. 23–32, available at https://www.b-ccentre.be/download/b-ccentre_legal/B-CCENTRE %20Van %20een %20netwerkzoeking %20naar %20online %20doorzoeking.pdf

Criminal Policy Service of the Ministry of Justice, reports in implementation of article 90*decies* CCP, available at http://www.dsb-spc.be/web/index.php?option=com_content&task=view&lang=nl&id=55

De Hert, Paul and Boulet, Gertjan, "The cooperation between Internet service/access providers and law enforcement authorities," country report (Belgium) for the Cybercrime Research Centre at Nicolaus Copernicus University (Poland), February 2015, 29 pp., available at http://www.cybercrime.umk.pl/files/files/Report%20Belgium_De%20Hert %20Boulet.docx [last accessed 10/2018].

De Hert, Paul and Gutwirth, Serge, *Anthologie privacy/Anthologie de la vie privée* (Anthology of privacy), Academic and Scientific Publishers, 2013, 64 pp., available at http://www.anthologieprivacy.be/sites/anthology/files/documents/anthologie-privacy-asp_0.pdf

De Hert, Paul and Boulet, Gertjan, "Cybercrime report for Belgium," *International Review of Penal Law (RIDP / IRPL)*, 2013, issue 84, no. 1–2, pp. 12–59, and *Electronic Review of the International Association of Penal* Law, 2013, available via http://www.penal.org/en/reaidp-2013-e-riapl-2013

De Hert, Paul and Vermeulen, Mathias, "Toegang tot sociale media en controle door politie. Een eerste juridische verkenning vanuit mensenrechtelijk perspectief" (Access to social media and control by the police: a first legal exploration from the human rights perspective), *Panopticon*, 2012, vol. 33(2), pp. 258–272.

De Hert, Paul, "C.A.O. no. 81 en advies no. 10/2000 over controle van Internet en e-mail" (Labour law: Soft law on e-mail and Internet practices), *Rechtskundig weekblad*, 2002-2003, vol. 66/33, 19 April 2003, pp. 1281–1294.

De Hert, Paul and Van Leeuw, Frédéric, "Cybercrime Legislation in Belgium," in Eric Dirix and Yves-Henri Leleu (eds.), *The Belgian reports at the Congress of Washington of the International Academy of Comparative Law*, Brussels, Bruylant, 2011, pp. 867–956, available at http://www.vub.ac.be/LSTS/pub/Dehert/389.pdf [last accessed 10/2018].

De Smet, Bart, "Voeging van strafdossiers op verzoek van de verdediging" (Adding a file at the request of the defence), *Rechtskundig Weekblad*, 2002–2003, p. 1022, annotation under Court of Appeal of Antwerp, 13 March 2002.

De Valkeneer, Christian, *Manuel de l'enquête pénale* (Manual on criminal investigation), Brussels, Larcier, 2006, 498 pp.

De Wolf, Daniel, "Rapport Belge" (Belgian report on criminal procedure), *Electronic Review of the International Association of Penal Law*, 2014, 52 pp., available at http://www.penal.org/sites/default/files/files/RA%20-%203.pdf

Dewandeleer, Dirk, "De kennisname van e-mails 'tijdens de overbrenging ervan', een verduidelijking van het telecommunicatiegeheim" (Taking knowledge of e-mails during the transmission phase. A clarification of the secrecy of telecommunications), annotation to the judgment of the Correctional Court of Leuven, 4 December 2007, *Tijdschrift voor Strafrecht*, 2008, vol. 3, pp. 226–231.

Dupont, Lieven, *Beginselen van strafrecht Deel 1* (Principles of criminal law vol. 1), Leuven, Acco, 2004, 229 pp.

European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.7.g, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

Federal Prosecutor's Office, Annual Report of the Public Prosecutor's Office to the Board of Prosecutors General for the period of 1 January 2012 till 23 December 2012, 2012, p. 124, available (in Dutch) at http://www.om-mp.be/images/upload_dir/jaarverslag2012.pdf [last accessed 10/2018].

Freyne, Thierry, "De bewaking van privécommunicatie en -telecommunicatie in strafonderzoeken: een stand van zaken" (The monitoring of private communications and telecommunications in criminal proceedings: a state of affairs), *Tijdschrift voor Strafrecht,* 2008, vol. 3, pp. 165–182.

Goossens, Franky, *Politiebevoegdheden en mensenrechten in België. Rechtsvergelijkend en internationaal onderzoek* (Police powers and human rights in Belgium. Comparative and international research), doctoral thesis, Leuven, 2006, 778 pp., available at https://lirias.kuleuven.be/bitstream/1979/420/2/frankydoctoraat.pdf

Kennes, Laurent, *Manuel de la preuve en matière pénale* (Manual on evidence in criminal matters), Mechelen, Kluwer, 2009, 443 pp.

Kerkhofs, Jan and Van Linthout, Philippe, *Cybercrime*, Politeia, Brussels, 2013, 639 pp.

Microsoft, "Law Enforcement Requests Reports", available at https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

National Labour Council, "National collective agreement no. 81 of 26 April 2002 on the protection of the private lives of employees with respect to controls on electronic on-line communications data", 26 April 2002, available via www.cnt-nar.be

Osula, Anna-Maria, "Remote search and seizure in domestic criminal procedure: Estonian case study," *International Journal of Law and Information Technology*, 2016, vol. 24, pp. 343–373.

Parliamentary preparatory works, Chamber of Representatives, regarding the improvement of the special investigation methods and certain investigation methods with respect to the internet and electronic and telecommunications, 2015-2016, no. 54 1966/001, 297 pp., available at http://www.dekamer.be/FLWB/PDF/54/1966/54K1966001.pdf

Parliamentary preparatory works, Chamber of Representatives, regarding international mutual assistance in criminal matters, 2003–2003, no. 51 1278/001, 53 pp., available at http://www.dekamer.be/FLWB/pdf/51/1278/51K1278001.pdf [last accessed 10/2018].

Parliamentary preparatory works, Belgian Chamber of Representatives, regarding special investigation methods and any other methods of investigation, 2001–2002, no. 50 1688/001, 193 pp., available via http://www.senate.be/www/?MIval=dossier&LEG=2&NR=1260&LANG=nl

Parliamentary preparatory works, Belgian Chamber of Parliaments, modifying the Act of 30 June 1994 protecting privacy against the interception of communication and telecommunication, 1996-1997, 29 May 1998, no. 49K1075/017, p. 10, available at http://www. dekamer.be/FLWB/PDF/49/1075/49K1075017.pdf [last accessed 10/2018].

Parliamentary preparatory works, Belgian Senate, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, 1993-1994, 18 May 1994, no. 843-2, 346 pp., available at http://www.senate.be/lexdocs/S0539/S05390364.pdf [last accessed 10/2018].

Parliamentary preparatory works, Belgian Senate, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, 1992–1993, 1 September 1993, no. 843-1, 67 pp., available at http://www.senate.be/lexdocs/S0539/S05390297.pdf

Pesquié, Brigitte (revised by Yves Cartuyvels), "The Belgian system", in Mireille Delmas-Marty and J.R. Spencer, *European Criminal Procedures*, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2002, pp. 81–141.

Schuermans, Frank, "Enkele (ver)nieuw(d)e politionele en strafvorderlijke onderzoeksmethoden" (Some (re)new(ed) police and criminal investigation methods), in Antoinette Verhage and Gert Vermeulen (eds.), *Mensenrechten en opsporing, terrorisme en migratie* (Human rights and detection, terrorism and migration), Maklu, Antwerp-Apeldoorn, 2017, pp. 15–38.

Traest, Philip, "Judicial control on the gathering and reliability of technical evidence in a continental criminal justice system", conference paper for the 16th International Conference of the International Society for the Reform of Criminal Law, 2002, 13 pp., available at http://www.isrcl.org/Papers/Traest.pdf [last accessed 10/2018].

Traest, Philip, "Rechts(on)zekerheid in materieel en formeel strafrecht en strafrechtelijk legaliteitsbeginsel" (Legal (un)certainty in material and formal criminal law, and the principle of legality in criminal law), *Rechtskundig Weekblad*, 1993–1994, pp. 1190–1207.

Voet, Stefaan, "Belgium's new specialized judiciary," *Russian Law Journal*, 2014, vol. II, Issue 4, pp. 129–145.

Van den Wyngaert, Chris, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, 1314 pp.

Verbruggen, Frank, Royer, Sofie and Severijns, Helena, "Reconsidering the blanket-data-retention-taboo, for human rights' sake?", *European Law Blog*, 1 October 2018, available at https://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/

Vermeulen, Gert, *Wederzijdse rechtshulp in strafzaken in de Europese Unie* (Mutual legal assistance in criminal matters in the European Union), Antwerp-Apeldoorn, Maklu, 1999, 632 pp.

Vermeulen, Gert, Vander Beken, Tom, De Busser, Els, Van den Wyngaert, Chris, Stessens, Guy, Masset, Adrien, and Meunier, Christophe, *Een nieuwe Belgisch wetgeving inzake internationale rechtshulp in strafzaken* (New Belgian legislation regarding international legal assistance in criminal matters), Antwerp-Apeldoorn, Maklu, 2002, 421 pp.

Verstraeten, Raf, *Handboek strafvordering* (Manual on criminal procedure), Antwerp, Maklu, 2007, 1193 pp.

Verstraeten, Raf and Verbruggen, Frank, *Straf- en strafprocesrecht voor bachelors* (Criminal law and criminal procedural law for bachelors), 11th revised edition, Antwerp-Apeldoorn, Maklu, 2018, 539 pp.

Vodafone, "Law Enforcement Disclosure Report," 2014, available at http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

The Washington Post, "Do France and Belgium have direct wiretap access to telecom switches?," 7 June 2014, available at http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/07/do-france-and-belgium-have-direct-wiretap-access-to-telecom-switches/

List of Abbreviations

ADIV	Algemene Dienst Inlichtingen en Veiligheid (General Intelligence and Security Service of the Armed Forces)
APA	Autonome Politionele Afhandeling (Traitement Policier Autonome/Autonomic Police Treatment)
APO	Ambtshalve Politioneel Onderzoek (Enquête Policière d'Office/Autonomic Police Treatment)
APT	Autonomic Police Treatment
BBI	Bijzondere belastinginspectie (Special Tax Inspectorate)
BIPT	Belgian Institute for Postal Services and Telecommunications
BELSPO	Federal Science Policy Office
BISC	Belgian Internet Service Center
CC	Criminal Code
CCP	Code of Criminal Procedure
CETS	Convention on Cybercrime
CFI	Cel voor Financiële Informatieverwerking (Belgian Financial Intelligence Processing Unit)
Comité P	Vast Comité van toezicht op de politiediensten (Comité permanent de contrôle des services de police/ Standing Police Monitoring Committee)
CJEU	Court of Justice of the European Union
CTIF	Cellule de Traitement des Informations Financières (Financial Intelligence Processing Unit)
DNS	Domain Name Service
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EJCN	European Judicial Cybercrime Network
ETSI	European Telecommunications Standards Institute
FOD	Federale Overheidsdienst (Federal Public Service)
ISI	Inspection spéciale des impôts (Special Tax Inspectorate)
ISP	Internet Service Provider
GDPR	General Data Protection Regulation
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
ITU	International Telecommunication Union
LEMF	Law Enforcement Monitoring Facility

MLAT	Mutual Legal Assistance Treaty
NNP	National Numbering Plan
NTSU-CTIF	National Technical & Tactical Support Unit – Central Technical Interception Facility
SIM-commission	Administrative Commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services
SGRS	Service général du Renseignement et de la Sécurité (General Intelligence and Security Service of the Armed Forces)
SPF	Service Public Fédéral (Federal Public Service)
Standing Committee I	Belgian Standing Intelligence Agencies Review Committee
VSSE	Veiligheid van de Staat/La Sûreté de l'Etat

Croatia*

National Rapporteurs:
Marko Jurić
Sunčana Roksandić Vidlička

* This report outlines the legislation and case law as of November 2018.

Contents

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Security Services with Powers of Telecommunications Interception

1. National security architecture

In Croatia, interception of content data is possible under two legal regimes, namely repressive criminal law and intelligence (or state security) law. Acquisition and use of what is commonly referred to as "traffic data" (see below chapter 4), including location data, is possible under repressive criminal law, intelligence (or state security) law and additionally under preventive police law.

There are several sources of law which apply to the surveillance of communications, including

- Constitution of the Republic of Croatia,[1]
- Electronic Communications Act (ECA),[2]
- Criminal Procedure Act (CPA),[3]
- Act on Security-Intelligence System of the Republic of Croatia (ASIS),[4]
- Police Duties and Power Act (PDPA),[5]
- Regulation on national security requirements of the Republic of Croatia for individuals and legal entities in telecommunications (NSR),[6]
- Criminal Code.[7]

The prerequisites for the surveillance of electronic communications differ between repressive criminal law, preventive police authority and intelligence.

---

[1] *Ustav Republike Hrvatske*, Official Gazette of the Republic of Croatia, no. 56/1990, 135/1997, 113/2000, 28/2001, 76/2010, 5/2014.

[2] *Zakon o elektroničkim komunikacijama*, Official Gazette of the Republic of Croatia, no. 73/2008, 90/2011, 133/2012, 80/2013, 71/2014, 72/2017.

[3] *Zakon o kaznenom postupku,* Official Gazette of the Republic of Croatia, no. 152/2008, 76/2009, 80/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017.

[4] *Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske,* Official Gazette of the Republic of Croatia, no. 79/2006, 105/2006.

[5] *Zakon o policijskim poslovima i ovlastima*, Official Gazette of the Republic of Croatia, no. 76/2009, 92/2014.

[6] *Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama*, Official Gazette of the Republic of Croatia, no. 64/2008, 76/2013.

[7] *Kazneni zakon,* Official Gazette of the Republic of Croatia, no. 25/2011, 144/2012, 56/2015, 61/2015, 101/2017.

2. Powers for the interception of telecommunications

a) Law of Criminal Procedure

Powers belonging to criminal law are strictly regulated (Arts. 332–340 CPA). There is a differentiation between interception of content data and acquisition of what is commonly referred to as traffic data. While older doctrine and case law considered that traffic data ("data about communications") fell outside the scope of private life, such data is increasingly seen as an integral part of a persons' private life, which merits protection via fundamental rights and freedoms. Legislative amendments made in recent years have sought to increase the level of legal protection for such data, by imposing more stringent standards for its acquisition and use. Notwithstanding these developments, the fact remains that there are still significant differences in the legal protection of traffic and content data, as will be explained below. While all relevant statutes are based on the premise that content data is necessarily part of an individual's private life, this is not always so with traffic data. Nevertheless, amendments of the CPA in 2013 and 2014 have made it clear that judicial authorization is now necessary to access traffic data for criminal justice purposes. Still, there are significant differences in the treatment of content data and traffic data under the CPA, most notably regarding conditions and safeguards under which this data can be obtained and used.

In Croatia, coercive powers in the field of criminal procedural law are delegated to state attorneys and to the police for interception of electronic communications.

b) Surveillance in the field of national security and intelligence law

The security and intelligence system of the Republic of Croatia consists of two security and intelligence agencies: the Security and Intelligence Agency (*Sigurnosno-obavještajna agencija*, SOA), and the Military Security and Intelligence Agency (*Vojna sigurnosno-obavještajna agencija*, VSOA). The activities of these agencies are bound by the Croatian Constitution, ASIS, NSR, the National Security Strategy, the Defence Strategy and the Annual Guidelines for the Work of Security Services. Their work is subject to scrutiny by the Croatian Parliament, the President of the Republic, the prime minister, ministers of defence and interior, the Office of the National Security Council and the Council for the civilian scrutiny of the security intelligence agencies.

SOA and VSOA have independent powers of surveillance, within their field of competence. Pursuant to Art. 33(3) ASIS, measures of secret information gathering include secret surveillance of telecommunications services, activity and traffic, namely:

a) secret surveillance of communication content,

b) secret surveillance of telecommunication traffic data,

c) secret surveillance of the location of the user,

d) secret surveillance of international telecommunications.

The most important operational role in the interception of communications lies with the Operational Technology Centre for the Surveillance of Telecommunications (*Operativno-tehnički centar za nadzor telekomunikacija*, OTC). OTC is a centre within the intelligence and security agency, responsible for activation and management of the measures of secret surveillance of telecommunications services. However, the OTC serves not only SOA and VSOA (intelligence agencies), but also the police and other bodies of criminal procedural law.

Legal and natural persons must, in cooperation with the OTC, ensure autonomous and exclusive access to the data concerned by the measures being applied. The competent supervisory and investigative bodies shall also be provided with access to the data required by the measures in question, in the framework of their legal powers.[8] Legal and natural persons are obliged to keep confidential data regarding the telecommunications transactions of the users of services, for one year.[9] Those persons are obliged to provide, at the request of the OTC, information regarding all means of communication that have appeared at a certain geographical, physical or logical location, regardless of the telecommunications (in)activity thereof, in the period of last 48 hours.

Obligations of the legal and the natural persons operating public telecommunications networks and providing public telecommunications and access services provided by the Act, relating to the function of secret surveillance are regulated in a Government regulation. The regulation on the obligations of legal and natural persons in field of national security in the area of telecommunications was adopted by the Government, at the proposal of the Council for the Coordination of Security Intelligence Agencies.[10]

The obligations of the Ministry of Defence and the Croatian Armed Forces provided by the Act relating to the function of secret surveillance, if they operate their own telecommunications networks, is laid down by the Minister of Defence at the proposal of Director of VSOA.[11]

---

[8] Art. 19 para. 4 of the Act.

[9] Art. 19 para. 5 of the Act.

[10] Art. 20 para. 1 of the Act.

[11] Art. 20 para. 2 of the Act. As provided in para. 3 of the same article, SOA and VSOA, in cooperation with other bodies authorised pursuant to the Criminal Procedure Act for the application of measures of secret surveillance of telecommunications, with the approval of the Council for the Coordination of Security Intelligence Agencies, adopt the rules and regulations regarding the technical requirements, the development of the appropriate technical equipment and programme support, questions relating to technical interfaces, and other matters relevant for the activation and the application of the measures of secret surveillance of telecommunications.

c) Surveillance in the field of police duties and powers

The Police are not empowered to conduct the interception of content data in the exercise of their duties and competences. They can only do so in the course of criminal proceedings, upon request and in accordance with the instructions given by the State Attorney and the courts.

Art. 68 PDPA empowers the police (1) to request analysis of "identity, duration and frequency of communications with specified communication addresses," (2) determination of "the location of communication devices" as well as location of "users of communication devices," as well as (3) "identification marks of communication devices." This power might be used for the purpose of (1) preventing and detecting criminal offences prosecuted ex officio and their perpetrators, (2) prevention of danger and violence, as well as (3) searching for persons and objects.

Application of Art. 68 PDPA does not require judicial authorization. Instead, it is based on the written approval of the Chief of the Criminal Police Administration or of the Chief of the National Police Office for the Suppression of Corruption and Organized Crime or of the Chief of Police Administration or by their replacement in case of absence.

In exceptional circumstances, namely when it is necessary to prevent immediate danger or violence or for the purpose of an urgent search for persons, the authorization may be given orally, but must be confirmed in writing within 24 hours of the oral approval.

Finally, application of Art. 68 PDPA is also subject to the principle of subsidiarity. Namely, this measure should be approved only on the basis of facts from which it is apparent that other actions could not or will not be able to attain the objective of the police work or if the achievement of that objective has presented unreasonable difficulties.

3. Responsibility for the technical performance of interception measures

As noted above, OTC is responsible for the operational execution of surveillance measures (including both interception of content data and acquisition of traffic data). To enable OTC to perform this function, communications service providers defined below are required to enable secret surveillance of their communications networks, and to establish direct connection lines to the OTC. In that sense, surveillance is not outsourced to private companies, but it requires their cooperation. The full scope of their cooperation obligations is analysed below. Finally, it must be emphasized that the OTC conducts surveillance on the whole territory of Croatia, and in all previously mentioned legal regimes (criminal procedural law, police duties, national security and intelligence gathering).

4. Legitimacy of data transfers between different security agencies

Various institutions responsible for these regimes and functions are separated from each other. The Croatian police are responsible for both prevention and repression, and the intelligence agency is responsible for intelligence gathering. However, both refer to OTC for technical support.

The results of interception measures obtained under the ASIS can be exchanged with the law enforcement in criminal proceedings. Pursuant to **Art. 56 ASIS**,

> Where the collected intelligence indicates that a criminal act which is prosecuted ex officio is being planned or committed, security and intelligence agencies shall notify State Attorney's Office thereon.
>
> The notification referred to in paragraph 1 of this Article may, by way of exception, include data regarding the manner in which the information was collected.
>
> The Directors of security and intelligence agencies may, suggest to the Chief State Attorney to postpone further actions within his/her scope of duty, if such actions might jeopardise the achievement of the objectives falling within the scope of activity of security and intelligence agencies, or endanger the safety of the employees and sources of security and intelligence agencies.

Intercepted data can be exchanged with competent authorities in other countries, in particular between intelligence agencies. This cooperation is regulated by Arts. 59 and 60 ASIS (see Annex I for the text of Articles in their entirety).

According to an SOA Report from 2017, SOA has been continuously developing close cooperation and building trust with other security and intelligence agencies. This cooperation takes place at various levels with respect to common interests and mutual security challenges. SOA has established bilateral cooperation and partnered up with selected agencies in order to build strategic relations and close cooperation at the highest degree of trust – joint operative actions and exchange of classified information. SOA is an active participant in multilateral forums and platforms, with particular emphasis on multilateral activities that are related to NATO and the EU. The Agency is a member of several multilateral initiatives and organizations, such as Counter Terrorist Group (CTG). SOA is a full member of CTG, along with security agencies of the EU member states, Norway, and Switzerland. The CTG focuses its activities on prevention and suppression of terrorism in European countries.[12]

B. Statistics on Telecommunications Interception

There is no obligation in the legislation for law enforcement authorities to report on the number of interceptions undertaken. Likewise, no such statistics are disclosed to the public.

---

[12] https://www.soa.hr/files/file/SOA-Public-Report-2017.pdf

II. Principles of Telecommunications Interception in Constitutional and Criminal Procedural Law

A. Constitutional Safeguards of Telecommunications

1. Areas of constitutional protection

There are several provisions of the Croatian Constitution pertaining to protection of communications and personal data, namely:

> **Article 35:** Respect for and legal protection of each person's private and family life, dignity, and reputation shall be guaranteed.
>
> **Article 36:** The freedom and privacy of correspondence and all other forms of communication shall be guaranteed and inviolable.
>
> Restrictions necessitated by the protection of national security and the conduct of criminal prosecution may be prescribed solely by law.
>
> **Article 37:** The safety and secrecy of personal data shall be guaranteed for everyone.
>
> Without consent from the person concerned, personal data may be collected, processed, and used only under the conditions specified by law.
>
> Protection of data and monitoring of the operations of information systems in the state shall be regulated by law.
>
> The use of personal data contrary to the express purpose of their collection shall be prohibited.

The Croatian Constitution therefore provides direct protection to communication privacy (Art. 36 paragraph 1), as well as to personal data (Art. 37). These provisions are directly applicable to all aforementioned statutes which regulate interception of content data and acquisition of traffic data. However, these rights are not absolute, and can be restricted in accordance with general constitutional rules and principles regarding limitations of constitutional rights (see below).

Moreover, it is worth noting that Croatia is a party state to the European Convention of Human Rights and Fundamental Freedoms (ECHR), and the Constitution prescribes the primacy of international treaties over domestic law, thus making Art. 8 ECHR, as well as the European Court of Human Rights' (ECtHR) case law an important tool when assessing the proportionality of limitations.

2. Principles of proportionality and necessity

Pursuant to **Article 16 of the Croatian Constitution**,

> Freedoms and rights may only be restricted by law in order to protect the freedoms and rights of others, the legal order, and public morals and health.
>
> Any restriction of freedoms or rights shall be proportionate to the nature of the need for such restriction in each individual case.

Therefore, all the aforementioned statutes which restrict the rights to privacy of (electronic) communications and data protection have to satisfy the standard three-part test in order to be deemed in line with the constitution. It is necessary that any restriction is done (a) by law, (b) in pursuit of a legitimate aim, and (c) is proportionate to the nature of the need in every individual case.

In the context of communications' surveillance, these conditions are observed, since restrictions are prescribed in written statutes which are accessible to the public and of necessary quality (in the sense that they are precise and foreseeable). Also, they pursue aims which are considered legitimate under the Constitution (investigation and prosecution of criminal offences, performance of police duties and powers, protection of national security and intelligence gathering). Finally, these acts usually implement certain conditions and safeguards and limit their application to what is considered necessary in particular context. These conditions are discussed below.

3. Other (non-constitutional) legal safeguards

Secrecy of communications enjoys protection in the context of criminal law. Firstly, Art. 143 Criminal Code provides protection against unauthorised audio recording and eavesdropping and Art. 146 Criminal Code prohibits unauthorised use of personal data (these two offences belong to the Chapter XIV of the Criminal Code, Crimes against Privacy) and Art. 269 of the same Code prohibits unauthorised interception of computer data (see Annex II for the text of Articles in their entirety).

According to statistical data of the State Attorney's office for the year 2017,[13] 308 adults, 15 younger adults and 10 juveniles were reported for committing Crimes against Privacy. The total of these offences under the Crimes Against Privacy Act (333) represents 0.9 % of the total number of all criminal offences committed by natural persons. Of these reports, 67 natural persons were reported for Unauthorised Audio Recording and Eavesdropping (Art. 143). 82.1 % of the reports of infringements of the Crimes Against Privacy were rejected. In the same period 50 cases for these offences were brought before the courts, from which 44 defendants were found guilty (success rate 88 %). Regarding Art. 269 (Unauthorised Interception of Computer Data), this offence belongs to Criminal Offences Against Computer Systems, Programs and Data (Chapter XXV of the Criminal Code), even fewer reports were filed. There were a total of 237 reports against natural persons (196 adults, 30 younger adults and 11 juveniles). These numbers represent an increase of 36 reports compared to 2016 (when 201 persons were reported). This increase is primarily due to the increase in reported adults by 23.3 %. Of

[13] The State Attorney's Report for 2017 (2018). Available online: http://www.dorh.hr/dorh07062018.

all offences, the most common is computer fraud (Art. 271 Criminal Code), for which 176 adults were reported (nearly 90% of all complaints against adults). However, when analysed against the total numbers of all criminal offences, these numbers are very insignificant.

B. Powers in the Code of Criminal Procedure

Among the coercive measures that can be applied to the suspect during the criminal procedure, one can distinguish between coercive measures designed to ensure the presence of defendant in the criminal proceedings and those intended to obtain evidence and objects which serve to establish the facts. The defendant is protected by several constitutional principles, above all the presumption of innocence (Art. 28 of the Croatian Constitution) which "represents the fundamental principle of regulating the relationship between individual and state repressive authorities." On the application of the measures of procedural coercion, i.e., regarding the interference in certain fundamental human rights or freedoms, only a court has the authority to decide on their implementation and these measures are restrictively applied following jurisprudence of the ECtHR: they must be prescribed by law, have a legitimate aim and be necessary in a democratic society. The last condition refers to the principle of proportionality, which in Croatian law is elevated to the constitutional level. Art. 16 paragraph 2 of the Constitution prescribes that any restriction on freedom or rights must be proportionate to the nature of the need for a limitation in each case. This means that any coercive measure must meet the criteria of suitability, necessity and proportionality. The CPA explicitly provides for the application of the principle of proportionality throughout the entire CPA. The general principle is stipulated in Art. 4 CPA: any act or measure restrictive of liberty or rights established by the CPA must be proportionate to the nature of the need for a limitation in each individual case. When deciding on acts and measures of limitation of freedom or ex officio, the court and other state bodies shall ensure that the burden of the measures is not applied if the same purpose can be achieved by a lesser measure. Their duration must be limited to the shortest necessary time.

Furthermore, *nullum crimen sine lege* is the main principle of Croatian criminal law,[14] and a constitutional principle (Art. 24). No one may be arrested or detained without a written court order grounded in law. Such an order has to be read and presented to the person placed under arrest at the moment of said arrest. The police authorities may arrest a person without a warrant when there is reasonable suspicion that such person has perpetrated a grave criminal offence as defined by law. Such person shall be promptly informed, in understandable terms, of the reasons

---

[14] In substantive criminal law, the principle "no crime without legal definition" requires *inter alia* that criminal statutes must be defined precisely by the legislator before the commission of a criminal act can be assumed.

for arrest and of his/her rights as stipulated by law. Any person arrested or detained shall have the right to appeal before a court, which must immediately decide on the legality of the arrest.

The principle of precise parliamentary enactment of public powers requires that all infringements of civil liberties must be based on precise laws. Coercive powers in the Croatian CPA are to a large extent based on differentiated, precise and specific provisions. Nevertheless, there are some ambiguities in the law, which will be analysed below.

III. Powers for Accessing Telecommunications Data in the Law of Criminal Procedure

A. Overview of the Legal Framework and the Respective Provisions in Criminal Procedural Law

In the field of criminal procedural law, interception of content data and accessing electronic communications data are regulated by the CPA, in particular Chapter XVIII, sections 12 and 13. In addition to the CPA, which contains the legal basis for interception of content data in Arts. 332 *et seq.*, the ECA regulates some aspects of the institutional framework necessary to conduct surveillance (namely, the obligation for electronic communications providers to cooperate with relevant state bodies). This Act also implements the data retention obligation for communications data, which subsequently enables relevant law enforcement authorities in the sphere of criminal procedural law to gain access to such data based on the CPA. Some operational and technical aspects of the surveillance system necessary to enable real-time interception of content data, are regulated by the ASIS and NSR.

It is also possible for law enforcement authorities to access some communications data using search and seizure. Provisions regulating search and seizure of stored computer data are regulated in the Arts. 257, 261 and 263 CPA.

All of these powers are discussed in detail below.

B. Interception of Content Data

1. Statutory provision

As noted above, interception of content data is regulated by Chapter XVIII, section 12 of the CPA. Within this section, Art. 332 regulates several so-called special investigative actions. **Art. 332 paragraph 1 CPA** reads as follows:

> **Article 332:** (1) If the investigation cannot be carried out in any other way, or that would be possible only with disproportionate difficulties, the investigating judge may,

upon the State attorney's written request containing statement of reasons, order against the person for whom there are grounds for suspicion the he or she has committed or has jointly with others taken part in committing an offence referred to in Article 334 of this Act, measures which temporarily restrict certain constitutional rights of citizens, namely:

1) monitoring and technical recording of telephone conversations and other means of remote technical communication;

2) interception, gathering and recording of computer data;

3) entry on the premises for the purpose of conducting surveillance and technical recording at the premises;

4) covert following and technical recording of individuals and objects;

5) use of undercover investigators and informants;

6) simulated sales and purchase of certain objects, simulated bribe-giving and simulated bribe-taking;

7) offering simulated business services or closing simulated legal business;

8) controlled transport and delivery of objects from criminal offences.

(2) […]

2. Scope of application

Art. 332 paragraph 1 sub-paragraph 1 CPA creates the legal basis for "monitoring and technical recording" of (a) telephone conversations and (b) other means of remote technical communication. Next, sub-paragraph 2 empowers authorities to conduct "interception, gathering and recording" of (c) computer data.

The notion of "telephone conversation" in sub-paragraph 1 is technology neutral. It therefore includes analogous and digital communication, as well as landline and mobile connections. Moreover, it is broadened by the second part of the same provision, which enables monitoring and recording of "other means of technical communication." These provisions certainly include communication between persons via IP systems.

The notion of computer data is not defined in the CPA. However, the definition in the Criminal Code (Art. 87 paragraph 13) can be applied here by analogy. Pursuant to this provision, "computer data" is defined as "any representation of facts, information or concepts in a form suitable for processing in a computer system."

To the best of our knowledge, issues regarding interception of content data in the communication between a person and cloud storage services, as well as between independent computer systems, have not been subject to court proceedings. In such circumstances, it is not possible to give a definite answer as to whether Art. 322(1) (1-2) would be applicable to such communication. However, while there might be some uncertainties about whether the provision covering surveillance of remote communications (sub-paragraph 1) or the provision for interception and collection of computer data (sub-paragraph 2) should be applied in particular circumstances, it is clear that these provisions are broad enough to cover different modes of com-

munication. Finally, there is no relevant legal distinction between interception based on sub-paragraphs 1 or 2 here.

From the provisions of the CPA, it is clear that Art. 331 should be applied in cases of instantaneous communication via telephone and other means of remote communication, as well as to interception of computer data. However, it not clear whether acquisition of content data which is stored during communication, for instance emails stored on the communication service provider's servers, should be accessed in accordance with Art. 322 or using the search and seizure provisions described below. To the best of our knowledge, this question has not been resolved in the case law.

3. Special protection of confidential communications content

The CPA contains some specific limitations and safeguards regarding privileged information in the context of interception. Furthermore, the Criminal Code prescribes the unlawful obtaining of secrets as an offence in several articles, namely: Art. 262 (Disclosure and Unauthorised Obtainment of a Business Secret), Art. 300 (Disclosure of Official Secret), Art. 347 (Disclosure of Secret Information), Art. 145 (Unauthorised Disclosure of a Professional Secret), Art 147 (Unauthorised Audio Recording and Eavesdropping).[15] The Croatian legislator is strict in prohibiting such unlawful and unauthorised information gathering. Some of the provisions however contain the exception clause, providing that such gathering of information could be deemed lawful and there is no criminal offence if the information gathering was done to protect the public interest. Since laws must be interpreted as a whole, in the case law it has sometimes been ruled that general limitations regarding persons who are exempt from the duty to testify are also applicable here, especially prior to the last couple of CPA amendments. The scope and status of persons exempted from the duty to testify is regulated by Art. 285 CPA (see Annex III).

The CPA explicitly contains specific safeguards in several articles, namely in Art. 64(1(5)), Art. 108 (7) and (8), Art. 186. In criminal proceedings, judicial protection is given as a form of control against potential abuses, including against unauthorised and unlawful communications interception. Among the specifically listed rights of defendant (Art. 64(1(5)), there is a right to communicate freely with defence counsel, without hindrance and on a confidential basis. In the process of apprehension, the arrestee has the right to speak freely and without any hindrance and supervision for up to thirty minutes to his defence counsel. If the arrestee has not retained a defence counsel or the latter cannot come, the arrestee must be given

[15] Refers to an attorney-at-law, notary public, health worker, psychologist, employee of a welfare institution, religious confessor or another person who discloses without authorisation a piece of information about personal or family life confided to them in the performance of their occupation.

the possibility to take a defence counsel from the list of attorneys on call from the Croatian Bar Chamber. Additionally, the arrestee has a right to communicate with a person of their choice, but that communication could be limited if deemed necessary in the interests of proceedings or other important interests (Art. 108(7) and (8). Art. 187, contains safeguards on collecting and processing personal data (see Annex IV).

4. Execution of telecommunications interception

In relation to the modes of interception, the CPA contains several basic provisions. Pursuant to Art. 335 paragraph 1 and Art. 337 paragraph 1, interception of content data is conducted by the police. In doing so, the police can either require access providers to extract and surrender certain communications or can obtain such information in cooperation with the operative-technical centre for the surveillance of communications (OTC). As explained above, although the OTC is part of the Security and Intelligence Agency and has no standalone role in criminal proceedings, it is authorised to conduct surveillance for the benefit of criminal proceedings, upon request.

Although both methods of conducting surveillance (ordering service providers to extract and submit data, as well as state authorities intercepting it autonomously) are legally possible, in practice, most interceptions are undertaken through the cooperation of the police and the OTC. In such circumstances, the OTC acts as the operative body which intercepts or otherwise obtains the relevant data by itself and without further assistance by service providers.

Both the individual service providers as well as the OTC are required to cooperate with the police and provide assistance necessary to obtain relevant data. In cases of failure to provide requested assistance to the police, the investigative judge can impose penalties of up to HRK 1 million (approximately EUR 133,000) to the service providers (as a legal entity), and up to HRK 50,000 (approximately EUR 6660) to the responsible natural person in the communication providers and the OTC.[16]

Other than few general provisions (power to intercept, duties to cooperate), the full range of OTC's technical capabilities in the interception of communications is not detailed in legislation, nor is otherwise disclosed to the public. There are also no specific rules regarding interception of communications to/from devices located in another country, or where the location of the device is unknown.

The CPA recognises the possibility of entry into the premises for the purpose of conducting surveillance and technical recording at the premises.[17] However, it ap-

---

[16] Art. 335(2) CPA.

[17] Art. 332(1)(3) CPA.

pears that, in the light of developing capabilities of the OTC to conduct surveillance autonomously, such auxiliary measures might be unnecessary.

Also, it is clear from other provisions of the CPA that "interception, gathering and recording of computer data" (on the basis of Art. 332(1)(2) can be achieved by remote access to a person's personal computer.[18]

Other accompanying measures are not defined in the law.

5. Duties of telecommunications service providers to cooperate

a) Addressees of duties to cooperate

To enable the OTC to perform surveillance autonomously, significant duties and obligations are imposed on the electronic communications service providers. There are no less than five statutes which impose these duties, namely the CPA, ECA, ASIS, PDPA, and the NSR. It is to be noted that many of their provisions are overlapping, and sometimes different terms are used to describe a certain notion. Also, relevant duties, while extensive, are also stipulated in relatively broad wording. All of this creates some of vagueness.

Pursuant to the CPA, surveillance orders are primarily directed against a specific person, and are executed by the police. As elaborated above, relevant providers are required to provide necessary assistance to the police. More commonly, the police cooperate with the OTC, which operatively executes the measure.

Regarding the service providers which might be subject to cooperation duties, different definitions are used. Firstly, the CPA stipulates that "telecommunication service providers" are required to provide necessary assistance to the police in the course of performing surveillance (without defining the notion of "telecommunication service provider").[19] However, the provisions of the ECA are broader and require cooperation with the OTC from all (a) "operators of public communication networks" and "publicly available electronic communication services."[20] Moreover, in the same context (cooperation with the OTC) ASIS uses the notions of "telecommunication services," "public telecommunication services," and "access services." Finally, the Regulation on national security requirements of the Republic of Croatia for individuals and legal entities in telecommunications (NSR), enacted on the basis of the ASIS, stipulates more precisely that natural and legal persons owning "public telecommunication network" and providing "public telecommunication services" and "access services" are (1) telecommunication operators, (2) network operators, (3) service providers, (4) access providers and (5) other entities designated by the law.

---

[18] Art. 332(3) CPA.

[19] Art. 335(2) CPA.

[20] Art. 108(1) ECA.

Unfortunately, it is not known to the public which of the different providers cooperate with the OTC pursuant to these provisions. There is no dispute that cooperation exists with providers of fixed and mobile telephone services, as well as providers of internet access services. The law is not clear on the issue whether infrastructure providers working on the IP-transport level, as well those providing communications services on the application level, could fall within the scope of the aforementioned provisions.

b) Scope of the duty to cooperate

The scope of the cooperation duties is defined in broad terms. For instance, pursuant to Art. 335(2) CPA, telecommunications providers are obliged to provide necessary "technical assistance" to the police. Provisions of the ECA, ASIS, and the NSR are more precise, but still drafted in very general terms.

First, pursuant to Art. 108(1) ECA, service providers mentioned above must establish and maintain, at their own expense, the "function of secret surveillance of electronic communications networks and services," as well as electronic communications lines to the OTC. This "function" is ensured by enabling the OTC to install necessary surveillance equipment and software into a service provider's communications systems,[21] and ensuring that the OTC's personnel has continuous and direct access to the locations and equipment necessary to enable surveillance.[22] The purpose of these duties is to ensure that the OTC has the possibility to execute surveillance orders autonomously (without further assistance from the service providers).[23]

Detailed instructions regarding hardware and software used, technical interfaces and other technical requirements necessary to enable surveillance are defined in the rules issued by the two security and intelligence agencies. These rules are not publicly available.

Second, Art. 108 ECA contains certain duties regarding encryption of data. Pursuant to its paragraph 7, if the communication service provider is compressing or encrypting electronic communications traffic, it must deliver such traffic data in its original (decrypted) form to the competent authorities. Moreover, it is stipulated that communications service providers must, "upon the request of the competent authorities referred to in paragraph 3 of this Article [bodies of criminal procedure law and security and intelligence agencies], prevent their users from using the programmes for encrypting the contents of the communication, or enable competent

---

21 Art. 19(1) ASIS.

22 Art. 19(2) ASIS.

23 Art. 19(3) ASIS.

authorities in executing decryption measures necessary to ensure secret surveillance […]."

Third, service providers must ensure that only the OTC has autonomous access to the data concerned by the active measures. Such access is also granted to competent supervisory and investigative bodies, in the exercise of their competences.[24]

Fourth, service providers are required to maintain secrecy about all equipment, procedures and data associated with surveillance mechanisms. Moreover, they must request and obtain appropriate security clearances for those of their employees who perform duties associated with the execution of surveillance measures.[25]

Fifth, the ECA imposes an obligation on providers of communications services to keep subscriber information. Pursuant to Art. 108(5) ECA, service providers "must keep a list of end-users of their services, which they are obliged to deliver to the competent authorities […] upon their request." Such list must contain "all the necessary data enabling unambiguous and immediate identification of every end-user."[26] Moreover, Ordinance on the Manner and Conditions for the Provision of Electronic Communications Networks and Services[27] stipulates that a subscriber contract has to contain, among other information, (1) name and seat for legal persons, or name and address for subscribers who are natural persons, (2) connection point address where the subscriber shall be provided with access to public communications network, (3) address for delivery of notifications and address for delivery of bills for provided electronic communications services, and (4) e-mail address at which the subscriber wants to receive notification in cases of contracted Internet access services.[28]

There are no legal rules covering technical aspects of the internet provider's transfer of intercepted data to authorities in a foreign country.

6. Formal prerequisites of interception orders

a) Competent authorities

Formal prerequisites for interception of content data are regulated by the Art. 332 paragraphs 1 and 2 CPA. As a general rule, interception is ordered by a written order of the investigating judge, issued upon the request of the State Attorney. Both the request and the order must contain a statement of reasons, including the necessity for applying the measure.

---

[24] Art. 19(4), ASIS, Art. 5 NSR.

[25] Art. 6 NSR.

[26] Art. 108(6) ECA

[27] Official Gazette of the Republic of Croatia, no. 154/2011, 149/2013, 82/2014, 24/2015, 42/2016.

[28] *Ibid.*, Art. 8(3)(1,7,8,9).

In exceptional circumstances, the State Attorney can issue an order himself. This is possible under two conditions: (1) there is a risk of delay, and (2) the State Attorney has reasons to believe that they will not be able to obtain a court order in due time. An Order issued by the State Attorney is valid for a period of 24 hours.[29] After issuing the order, the State Attorney must submit it to the investigating judge within 8 hours. Moreover, he must submit a written memorandum explaining the reasons for issuing it, as well as stipulating whether it is necessary to continue with the application of surveillance. Once he receives the order and the explanation from the State Attorney, the investigating judge is required to rule on the legality of that order immediately.[30] In particular, the judge must decide whether all the legal requirements have been observed, and whether there was indeed a risk in delaying the initiation of the measure.

If the investigating judge does not accept the explanation of the State Attorney, they must request that the final decision be made by a panel of judges, and the State Attorney's order shall continue to be valid until the panel reaches this decision. Pursuant to Art. 332(5) CPA, the panel must make the decision within 12 hours of receiving the request from the investigating judge.

b) Formal requirements for the application

There are no specific formal requirements for the application to conduct surveillance. As explained above, the State Attorney must submit a written application containing a statement of reasons. This application must contain sufficient facts for the judge to conclude that the investigation cannot be carried out in any other way, or an alternative would be possible only with disproportionate difficulties.

c) Evidence on the basis of which the applicant's case is presented to the court

The State Attorney's case is presented to the investigating judge on the basis of submission of investigative files.

7. Substantive prerequisites of interception orders

a) Degree of suspicion

Pursuant to Art. 332(1) CPA, the relevant standard is "grounds for suspicion."

---

[29] Art. 332(2) CPA.

[30] Art. 332(5) CPA.

b) Predicate offences

Offences for which interception of content data can be ordered are essentially grouped into three categories.

The first category includes (1) all criminal offences punishable by long-term imprisonment, and (b) the following offences: war crimes (Art. 91 paragraph 2), terrorism (Art. 97 paragraphs 1, 2 and 3), financing of terrorism (Art. 98), training for terrorism (Art. 101), terrorist association (Art. 102), slavery (Art. 105), trafficking in human beings (Art. 106), trafficking in human body parts and human embryos (Art. 107), unlawful deprivation of liberty (Art. 136, paragraph 4), kidnapping (Art. 137 paragraph 3), sexual abuse of a child under the age of fifteen (Art. 158), child pandering (Art. 162 paragraphs 1 and 3), exploitation of children for pornography (Art. 163, paragraphs 2 and 3), serious criminal offences of child sexual abuse and exploitation (Art. 166), money laundering (Art. 265 paragraph 4), abuse of position and authority (Art. 291 paragraph 2) if the offence was committed by an official person, taking a bribe (Art. 293) if the offence was committed by an official person, trading in influence (Art. 295) if the offence was committed by an official person, criminal association (Art. 328), committing a criminal offence as a member of a criminal association (Art. 329 paragraph 1, items 3 through 6), murder of an internationally protected person (Art. 352), kidnapping of an internationally protected person (Art. 353), for the criminal offences against the Republic of Croatia (Title XXXII) and against the Armed Forces of the Republic of Croatia (Title XXXIV) punishable by imprisonment for a term of at least five years and for all criminal offences punishable by long-term imprisonment.

The second category includes the following offences: genocide (Art. 88 paragraph 3), crime of aggression (Art. 89 paragraphs 2 and 3), command responsibility (Art. 96), recruitment for terrorism (Art. 100), preparing criminal offences against values protected under international law (Art. 103), torture and other cruel, inhuman or degrading treatment or punishment (Art. 104) if committed against a child, murder (Art. 110), unlawful deprivation of liberty (Art. 136 paragraph 3), kidnapping (Art. 137), prostitution (Art. 157 paragraph 2), sexual abuse of a child over the age of fifteen (Art. 159), child enticement for the purpose of satisfying sexual needs (Art. 161), child pandering (Art. 162), exploitation of children for pornography (Art. 163), exploitation of children for pornographic performances (Art. 164), abduction of a child (Art. 174 paragraph 3), unauthorised manufacture of and traffic in illicit drugs (Art. 190 paragraphs 2, 3 and 4), serious criminal offences against general safety (Art. 222), attack on an aircraft, vessel or immovable platform (Art. 223), robbery (Art. 230 paragraph 2), extortion (Art. 243 paragraphs 4, 5 and 6), receiving bribes in business dealings (Art. 252), misuse of public procurement procedures (Art. 254), avoidance of customs controls (Art. 257), subsidy fraud (Art. 258), money laundering (Art. 265), counterfeiting money (Art. 274), abuse of position and authority (Art. 291), unlawful favouritism (Art. 292), taking a

bribe (Art. 293), giving a bribe (Art. 294 paragraph 1), trading in influence (Art. 295), illegal entry into, movement and residence within the Republic of Croatia (Art. 326 paragraph 2) and committing a criminal offence as a member of a criminal association (Art. 329).

The third category includes the following offences: public incitement to terrorism (Art. 99), unlawful deprivation of liberty (Art. 136), non-consensual sexual intercourse (Art. 152), rape (Art. 153), serious criminal offences against sexual freedom (Art. 154), prostitution (Art. 157), abduction of a child (Art. 174), neglect and abuse of the rights of a child (Art. 177), falsification of medicinal products or medical devices (Art. 185), unauthorised manufacture of and traffic in illicit drugs (Art. 190), enabling the use of illicit drugs (Art. 191, paragraphs 2 and 3), unauthorised manufacture of and traffic in substances banned in sports (Art. 191a), extortion (Art. 243), receiving or giving bribes during bankruptcy proceedings (Art. 251), giving bribes in business dealings (Art. 253), producing, procuring, possessing, selling or giving to another for use forgery tools (Art. 283), giving a bribe (Art. 294), giving a bribe for trading in influence (Art. 296), disclosure of official secret (Art. 300) if the offence represents a violation of the secrecy of the inquiry and fact-finding activity, giving false testimony (Art. 305), preventing the presentation of evidence (Art. 306), violation of secrecy of proceedings (Art. 307) if the offence represents a violation of secrecy in criminal proceedings, disclosing the identity of a person in danger or protected witness (Art. 308), coercion against a judicial official (Art. 312), illegal entry into, movement and residence within the Republic of Croatia (Art. 326), unlawful possession, making and procurement of weapons and explosive substances (Art. 331), murder of an internationally protected person (Art. 352), kidnapping of an internationally protected person (Art. 353), attack on an internationally protected person (Art. 354), threat to an internationally protected person (Art. 355) and for criminal offences against computer systems, programmes and data (Title XXV) and against intellectual property (Title XXVII) if committed by the use of computer systems or computer networks.

c) Persons and connections under surveillance

Generally, the primary subject of the interception order is the suspect, or more precisely, the person against whom there are grounds for suspicion that they have committed or jointly with others, taken part in committing one of the serious criminal offences listed above.

In addition to the suspect, surveillance can be ordered for those persons against whom there are grounds for suspicion that: (1) they have delivered to, or received from the perpetrator of the offences, […] information and messages in relation to offences, or (2) the perpetrator has used their telephone or other telecommunications devices, or (3) they have hidden the perpetrator of the criminal offence or helped him prevent being discovered by hiding the means by which the criminal

offence was committed, traces of the criminal offences or objects resulting or acquired through the criminal offence or in any other way.

Also, pursuant to Art. 332(9) CPA, "in case there is no knowledge about the identity of the accomplices in the criminal offence, the measure referred to in paragraph 1 item 8 of this Article may be determined in accordance with the object of the criminal offence."

The CPA does not require the likelihood that the anticipated evidence will be obtained by means of the requested interception as one of the substantive conditions.

d) Subsidiary application of the measure

The CPA does not contain an obligation that less intrusive measures first be tried unsuccessfully, since it is, pursuant to Art. 332(1), sufficient that alternative measures would be unacceptably burdensome.

e) Proportionality

There is no standalone requirement of proportionality in regard to the seriousness of an offence in the individual case. On the contrary, it is only necessary to prove that investigation cannot be undertaken otherwise, and that the offence in question is one from the list of predicate offences (see above).

f) Consent to interception

When the person concerned consents to the interception, it is still necessary to satisfy previously mentioned conditions regarding necessity and predicate offences. In any case, an interception order must always be granted in accordance with the CPA.

8. Validity of interception orders

a) Maximum length of interception orders

In normal circumstances, interception orders can be made initially for a period of up to three months. In emergency cases, as explained above, the State Attorney can order the interception himself (for a period of 24 hours) and must then seek and obtain confirmation of that order from the investigating judge or the panel of judges. In any case, after the initial period of 24 hours, interception can continue only on the basis of a judicial order for a period requested by the State Attorney and granted by the court, but no longer than three months.

b) Prolongation of authorisation

After the expiry of the initial three-month period, interception can be extended for another three months, provided that (1) the measure is showing positive results, and (2) there are reasons to continue with its application. Another extension, after the period of six months, is possible only in investigations of criminal offences from the first and second category (described above). Finally, interception during investigations of the most serious crimes (from the first category) can be extended for another six months, up to a total of 18 months.[31]

The procedure for renewal of interception is essentially the same as for its initial application. The State Attorney will submit an application to the investigating judge; in the case where investigating judge concludes that there are no reasons to prolong the interception the State Attorney can submit an appeal (within eight hours) to the panel of judges, and the panel must rule in the next 12 hours.

c) Revocation of authorisation

Notwithstanding the periods for prolongation mentioned above, duration of the interception order is limited by general requirements of necessity and subsidiarity. Therefore, interception must be revoked by the investigating judge if and when the general conditions for its application are no longer present.[32]

If the interception reveals information pointing to the commission of another offence (which was not covered by the interception order), that part of the record shall be copied and sent to the State Attorney if it pertains to one of the offences for which interception can be ordered (see above). There is no obligation to halt the interception in such a case.

9. Duties to record, report, and destroy

As noted above, interception is executed by the police (usually in cooperation with the OTC). Pursuant to Art. 337(1) CPA, the police have the obligation to draw up daily reports about the application of the interception order and document technical recordings. These are delivered to the State Attorney upon his request.

Moreover, the investigating judge has the right to request from the State Attorney, at any time, a report on the progress of the interception and an elaboration of the need for its continued application. He must request this report and elaboration after every three months (in cases when interception was prolonged for a period of

---

[31] Art. 335(3) CPA.

[32] Art. 335(4) CPA.

six months). Also, the investigating judge can request daily reports and technical recordings from the police whenever he deems necessary.[33]

After the termination of the interception, the police prepare a final report, which must include (1) time of the commencement and the termination of the interception, and (2) number and identity of persons covered by the measure. The police will also make two copies of the technical recording; one of which will remain archived with the police and the second will be delivered to the State Attorney.

Pursuant to Art. 335(4) CPA, "if the State Attorney desists from prosecution or if the data and information obtained by the application of the measures are not relevant for proceedings, they shall be destroyed under the supervision of the investigating judge, who will draw up a separate record thereon."

10. Notification duties and remedies

a) Duty to notify persons affected by the measure

The Croatian CPA contains no duty to inform intercepted persons about interception.

b) Criminal consequences of unlawful interception measures

Unauthorised interception is a criminal offence, punishable in accordance with Art. 143 Criminal Code (see Annex II).

For the frequency of this offence in practice see statistical information provided in Section II.A.3. above.

b) Independent supervision

There is no independent supervision mechanism for interception measures within the CPA framework.

11. Confidentiality requirements

The CPA contains no specific obligations for communications service providers to keep their supportive measures confidential. On the other hand, the NSR stipulates that all communications service providers are obliged to treat all information and knowledge about secret surveillance systems as confidential, in accordance with the Information Secrecy Act.

---

[33] Art. 337(1) CPA.

Pursuant to Art. 118(1) ECA, failure to provide assistance to the OTC in the interception measures is subject to misdemeanour penalties of up to 10 % of annual turnover for communications service providers, and up to HRK 100,000 (approximately EUR 13,333) for responsible natural persons.

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

a) Collection of traffic data

aa) Relevant information

To begin, it is important to note that in Croatia communications service providers are obliged to retain traffic data (see below 4.1.6.), as well as to keep a list of end-users (subscriber information, see below 4.1.5.). Access to this data is possible in accordance with the CPA (for criminal justice purposes), ASIS (for national security and intelligence purposes) and the PDPA (for some police duties). These statutes contain different conditions and safeguards for accessing traffic and subscriber information. In this chapter, we only assess conditions under the CPA (criminal justice purposes).

The legal basis for accessing traffic data in criminal proceedings is found in Art. 339.a CPA ("Analysis of telecommunication contacts"). This article was added to the CPA in 2013, with the express purpose of enhancing the level of protection of privacy and personal data vis-à-vis traffic data.[34] Moreover, it was once again amended in 2014, when the list of criminal offences for which this measure can be applied was narrowed down. Pursuant to Art. 339.a, a State Attorney can request (1) analysis of "identity, duration and frequency of communications between the user of a registered communication device and specified communication addresses," (2) determination of "the location of communication devices" as well as location of "users of communication devices," and (3) "identification marks of communication devices." These measures are executed by the police, through the OTC.

In relation to accessing subscriber information, Art. 263 CPA is relevant. Pursuant to its provisions, "subscription information" (among other categories of data) must be handed over to the State Attorney upon his written request. Upon receiving such order, whoever is in possession of such data (typically telecommunications service providers) is required to produce it "in an integral, original, legible and understandable format."[35]

---

[34] Proposal for amendment of CPA in 2013, pp. 138–139.

[35] Art. 263(2) CPA.

bb) Substantive prerequisites of collection

Pursuant to Art. 339.a CPA, analysis of telecommunications contacts can be performed against (a) the registered owner or user of a communication device, or (b) against a person associated with the person under suspicion. This measure can be performed only if certain substantive prerequisites have been fulfilled. First, there must exist a suspicion that a user of a device (or one associated with this user) has committed criminal offences.[36] Second, this criminal offence must be serious enough to trigger the application of this measure. Pursuant to the CPA, offences for which analysis of traffic data can be ordered include all those which might give rise to interception of content (see above), as well as all other offences punishable by imprisonment of more than five years.

cc) Formal prerequisites of collection

Analysis of telecommunications contacts can only be applied (1) on the basis of an order, or (2) with the written consent of the person concerned.[37]

In ordinary circumstances, an order is issued by an investigating judge, following a written and reasoned motion by the State Attorney.[38] Upon receiving such a motion, the investigating judge is required to rule on it within four hours.[39] In exceptional circumstances, where there is a risk of delay and the State Attorney has reasons to believe that they will not be able to obtain a court order in due time, they can issue the order directly. If that is the case, the State Attorney is required to submit the order and a written memorandum explaining the reasons for it to the judge, within 24 hours, and the judge must rule on the legality of that order within 48 hours. If the data about communications has been obtained without a judge's order, or if the order made by State Attorney did not receive judicial approval in due time, the data cannot be used as evidence.[40]

dd) Procedure for disclosure of data

The Police obtain traffic data through the OTC, using the integrated surveillance system described above.

---

[36] Measure is applicable for all criminal offences punishable by imprisonment for a term of more than five years, and some other offences explicitly enumerated in the CPA.

[37] Art. 339.a(8) CPA.

[38] Art. 339.a CPA.

[39] Art. 339.a(3) CPA.

[40] Art. 339.a(9) CPA.

b) Collection of subscriber data

aa) Relevant information and prerequisites

Pursuant to Art. 108(5) ECA, communications service providers are required to keep a list of end-users of their services, and to deliver this information to competent authorities in, *inter alia*, the criminal justice arena, upon their request. This obligation is further regulated in the CPA, which stipulates in Art 263 that certain computer data, including subscription information, must be handed over to the State Attorney upon his written request. While the term "subscription information that [is] in possession of the service provider"[41] is not defined in the CPA, to the best of our knowledge this shortcoming does not lead to any problems in practice.

Upon receiving an order in accordance with Art. 263 CPA, whoever is in possession of such data is required to produce it "in an integral, original, legible and understandable format."[42] In the written order to produce data or subscriber information, the State Attorney will stipulate a term for compliance with it.[43] Anyone who, without justified cause, fails to comply with the production order within that term may be subject to a fine of up to HRK 50,000 (approximately EUR 6666). Further failure to comply (after the imposition of a monetary penalty) might lead to imprisonment of up to one month.[44]

There are several conditions and safeguards which limit the application of this measure.

First, an order to produce "objects," which includes computer data and subscriber information, *cannot be applied against certain persons*.[45] These include (1) the defendant, and (2) persons who are exempt from the duty to testify.[46]

Second, when obtaining data or information on the basis of Art. 263 CPA, it is necessary to note that fact in the record, and to issue a receipt for objects that are handed over.

Finally, data and information obtained contrary to the provisions of Art. 262(1) CPA cannot be used as evidence in criminal proceedings.[47]

---

41 Art. 263(1) CPA.

42 Art. 263(2) CPA.

43 Art. 263(2) CPA.

44 Art. 263(2) CPA in conjunction with Art. 259(1).

45 Art. 261(4) CPA.

46 Scope and status of persons exempted from duty to testify is regulated by Art. 285 CPA (see Annex III).

47 Art. 262(7) CPA.

bb) Dynamic IP-addresses

Attributions of a dynamic IP-address and its connection with the actual user fall within the scope of data retention obligations, as described below (4.1.6.). This information can be obtained by the police through the OTC, in accordance with Art. 339.a CPA (described above).

c) "Data retention"

aa) Retention of subscriber information

Croatian law imposes an obligation on providers of communication services to keep subscriber data. Pursuant to Art. 108(5) ECA, service providers[48] "must keep a list of end-users of their services, which they are obliged to deliver to the competent authorities […] upon their request." Such list must contain "all the necessary data enabling unambiguous and immediate identification of every end-user."[49]

Moreover, the Ordinance on the Manner and Conditions for the Provision of Electronic Communications Networks and Services[50] stipulates that a subscriber contract has to contain, among other information, (1) name and seat for legal persons, or name and address for subscribers who are natural persons, (2) connection point address where the subscriber shall be provided with access to public communications network, (3) address for delivery of notifications and address for delivery of bills for provided electronic communications services, and (4) e-mail address at which the subscriber wants to receive notification in cases of contracted Internet access services.[51]

In practice, almost all service providers will also require a Personal Identification Number of a person to conclude a subscription contract. However, it is necessary to note that in the Republic of Croatia there is no legal obligation to register SIM cards and it is possible to procure such cards without providing any personal data. However, if pre-paid services are procured directly from service providers, most of them will collect some personal information about the user. Finally, some subscriber information is also subject to retention obligations. Consequently, service providers are required to retain, on the basis of NSR, (1) name and surname of a natu-

---

[48] For the purposes of this act, service providers include "operators of public communications networks and publicly available electronic communications services, as well as legal and natural persons, which, pursuant to specific regulations, install, use or offer for use electronic communications network or provide electronic communications services in the territory of the Republic of Croatia".

[49] Art. 108(6) ECA.

[50] Official Gazette of the Republic of Croatia, no. 154/2011, 149/2013, 82/2014, 24/2015, 42/2016.

[51] *Ibid.*, Art. 8(3)(1, 7, 8, 9).

ral person or name of a legal person who are subscribers or registered users, and (2) their addresses.[52]

bb) Retention of traffic data

Croatia operates mandatory retention mechanisms for communications traffic data. The retention period is 12 months. Collection and use of traffic data for criminal justice purposes is regulated by the CPA, ECA, ASIS, and the NSR. It must be emphasised that data retention has multiple purposes in Croatia, since the information can be used for (a) criminal justice purposes, (b) the exercise of police duties and powers, and (c) national security and intelligence purposes.

It must be emphasised that some terminological confusion is possible here. The notion of "traffic data" is used only in Electronic Communications Act (ECA), which is harmonised with the EU Directive on privacy and electronic communications. "Traffic data" is therefore defined as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the calculation and billing thereof."[53] When authorising the use of the data in question, relevant statutes use different terminology. Therefore, in the field of police affairs, PDPA provides for a power to gain access to and to analyse (1) "identity, duration and frequency of communications" between the user of a registered communication device and specified communication addresses, (2) "location of communication devices" and (3) "identification marks of communication devices."[54] Identical language is used in the CPA (Art. 339.a). Finally, in the field of national security and intelligence, ASIS authorises the Security and Intelligence Agency (SIA) and Military Security and Intelligence Agency (MSIA) to gain access to "data about telecommunication traffic" and to the "location of the user."[55] In this chapter, we use these notions as well as the overall and widely accepted term "traffic data" interchangeably.

The ECA and ASIS both contain a data retention obligation as a fundamental rule, which is essentially the same in both statutes. A detailed list of data which must be retained is specified in the NSR. This list is the same as the one in the (now invalidated) EU Data Retention Directive. It should be noted that, notwithstanding the judgments of the CJEU in the *DRI* and *Tele2/Watson* cases, there have been no significant changes in the data retention system of Croatia in recent years. On the other hand, provisions of the CPA were amended in 2013 and 2014 in order to provide enhanced safeguards in the use of traffic data for criminal justice purposes.

---

52 Arts. 21 and 22 NSR.

53 Art. 2(1)(55) ECA.

54 Art. 68(1-2) PDPA.

55 Art. 33(3)(1)(b-c) ASIS.

To begin with, a data retention obligation is imposed on the basis of the ECA which prescribes, in **Art. 110(1)**, that service providers must retain data necessary to

> (1) trace and identify the source of a communication, (2) identify the destination of a communication, (3) identify the date, time and duration of a communication; (4) identify the type of communication, (5) identify users' communication equipment or what purports to be their equipment, and (6) data necessary to identify the location of mobile communication equipment.

Similarly (and more generally), the ASIS stipulates in Art. 19(5) that communications service providers are required to retain "data about telecommunication traffic." While this term is left undefined in the ASIS itself, the scope of the retention obligation is extensively regulated in the secondary statute, namely the NSR. Pursuant to Arts. 17–25 NSR, communications service providers must retain the following data: data necessary to trace and identify the source of a communication, data necessary to identify the destination of a communication, data necessary to identify the date, time and duration of a communication, data necessary to identify the type of communication, data necessary to identify users' communication equipment or what purports to be their equipment, and data necessary to identify the location of mobile communication equipment (see Annex V).

All of the above-mentioned information is retained for a period of one year.

2. Identification of the device ID of a mobile end terminal and its card number

Device IDs as well and card numbers in mobile telecommunication services are "data necessary to identify users' communication equipment" and are retained in accordance with the ECA, ASIS and the NSR. They can be obtained by the police through the OTC, in accordance with Art. 339.a CPA (described above).

D. Access to (Temporarily) Stored Communications Data

1. Online-search by remote forensic software (including specialised norms on source electronic communications interception)

There are no detailed provisions regulating this procedural power in the Croatian legislation. Regarding the use of remote forensic software, the CPA stipulates only indirectly that the special investigative action of "entry on the premises for the purpose of conducting surveillance and technical recording at the premises" might include remote access to the computer of the suspect, if that computer is located within their home.[56] There are no provisions in the CPA regarding the methods which might be used, data which can be accessed, or territorial scope. In terms of

[56] Art. 332(1,3) CPA.

other conditions and safeguards, entry on the premises is considered one of the special investigative actions, applicable under the same conditions and safeguards as the interception of content data.

2. Search and seizure of stored communications data

a) Relevant provisions

It is still an open question whether acquisition by law enforcement authorities of electronic communications data which is stored (i.e., on internet service provider's servers) should be done in accordance with the rules regarding interception of content, or by application of the rules regarding search and seizure. In the opinion of the authors the latter approach is appropriate.

The CPA stipulates in Art. 257(1) that the search of movable property extends to (1) computers, (2) devices connected to the computer, (3) other devices for collecting, saving and transfer of data; telephone, computer and other communications and (4) data carriers (mediums). In several decisions, the Supreme Court has upheld the practice of searching various electronic devices based on Art. 275 CPA.[57]

Regarding seizure of computer data, Art. 257(1) CPA states that "upon the request of the authority carrying out the search, the person using the computer or having access to the computer or data carrier or the telecommunications service provider shall provide access to the computer, device or data carrier and give necessary information for an undisturbed use and the fulfilment of search objectives." If a person, other than the defendant, fails to provide such access or gives information without justified cause, they may be penalised by the investigating judge upon the motion of the State Attorney, first with a monetary penalty of up to HRK 50,000 (approximately EUR 6666), and, in cases of further non-compliance, with one month of imprisonment.[58]

Also, as was noted above, once the search order is issued, the authority carrying out the search is empowered to request the previously mentioned persons to immediately undertake measures for preventing the destruction or modification of data. Failure to comply with such a request might lead to the same sanctions as described above.

---

[57] For example, in its recent decision I Kž-Us 58/15-4 of 12 May 2015 the Supreme Court confirmed that Art. 257 can be validly applied as a legal basis to search computer and data on the hard drive.

[58] Art. 257/1 CPA.

b) Conditions and safeguards

In order to properly execute a search, the relevant authorities are required to follow a number of procedures, conditions and safeguards defined in the CPA:

1. A search for computer data can only be conducted if such data is important for the criminal procedure, and it is probable that it might be found within a certain computer system.[59]
2. A search is conducted on the basis of an order, issued by the investigating judge, upon the request of the State Attorney. A search order must be written and contain a statement of reasons. It must designate the object of a search with precision.[60] Furthermore, the purpose of a search must be explained, and the authority to conduct it (State Attorney, the investigator or the police) indicated in the order.[61]
3. The investigating judge is required to rule on the State Attorney's request for a search within 4 hours. If the request has been denied, the State Attorney is entitled to an appeal within 8 hours, upon which the panel will decide within 12 hours.[62]

Seizure of computer data obtained in the course of a computer search is done on the basis of Arts. 261–263 CPA. An ordinary application of these provisions, in conjunction with the search measure, will lead to the situation where the computer system itself, together with the data contained, is seized. By way of exception, Art. 263(3) provides that data which is not related to the criminal offence for which the action is taken, and which is furthermore needed by the person against whom the measure is applied, "may be recorded to an appropriate device and be returned to this person even prior to the conclusion of the proceedings."

3. Duties to cooperate: production and decryption orders

There are no general provisions in the Croatian legislation which would impose a duty to decode encrypted data, or to produce necessary information to do so (i.e., passwords). On the other hand, such obligation exists in the course of search and seizure, pursuant to Art. 257(1) CPA. As noted above, **Art. 257(1) CPA** stipulates that

> upon the request of the authority carrying out the search, the person using the computer or having access to the computer or data carrier or the telecommunications service pro-

---

[59] Arg. ex., Art. 240(2) CPA.

[60] For example, courts have in one case declared that the search of a memory card, found together with a computer, is invalid (and therefore inadmissible), due to the fact that the search warrant was issued only for a computer and not also for the card. See the decision of the Croatian Supreme Court, no. III Kr 165/2011-5 of 19 September 2012.

[61] Art. 242(1,7) CPA.

[62] Art. 242(2) CPA.

> vider shall provide access to the computer, device or data carrier and give necessary information for an undisturbed use and the fulfilment of search objectives.

Failure to provide such access or giving information without justified cause may be penalised by the investigating judge upon the motion of the State Attorney, first with a monetary penalty of up to HRK 50,000 (approximately EUR 6666), and, in cases of further non-compliance, with one month of imprisonment.[63] However, this penalty cannot be imposed on the defendant.[64]

IV. Use of Electronic Communication Data in Judicial Proceedings

Pursuant to **Art. 333(1) CPA**,

> Recordings, documents and objects obtained by the application of the measures referred to in Article 332 paragraph 1 item 1 to 8 of this Act may be used as evidence in criminal proceedings.

There are no specific rules regarding the admissibility of intercepted or stored electronic communications data as evidence in criminal proceedings. Intercepted communications are one of the sources of evidence and are treated pursuant to general rules and principles regarding evidence. Intercepted material can be introduced in the form of audio and/or video recordings, other recordings as well as transcripts.

Non-observance of formal and substantive prerequisites can render the intercepted material inadmissible. Pursuant to **Art. 335(7) CPA**,

> if the measures referred to in Article 332 of this Act are undertaken contrary to the provision of Article 332 of this Act, the evidence deriving from the data and information obtained in this manner may not be used as evidence in the criminal proceedings.

Pursuant to Art. 335(6) CPA, intercepted data can be used for the prosecution of individuals who were not the subject of the underlying interception order, provided that information and data obtained in that way pertains to one of the criminal offences for which it is possible to order interception in the first place. On the other hand, intercepted data obtained from outside the criminal justice system (in accordance with the ASIS) cannot be admitted as evidence in criminal proceedings.

---

[63] Art. 257/1 CPA.

[64] Art. 257(3) CPA.

V. Exchange of Intercepted Electronic Communications Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

The legal basis on mutual legal assistance applicable for the interception of electronic communications in the Republic of Croatia is the Criminal Procedure Act together with multilateral treaties, bilateral treaties and the European Investigation Order. The latter depends on the requested or requesting state for mutual legal assistance. Namely, in Art. 332 CPA there are clearly prescribed prerequisites for the interception, gathering and recording of electronic data, persons authorised to conduct such operations and the manner in which such interception of electronic communications must be carried out. Therefore, if the investigation cannot be carried out in any other way or would be accompanied by great difficulties, the judge of the investigation may, upon a written request with a statement of reasons from the State attorney, make an interception order relating to the person against whom there are grounds for suspicion of committing or taking part in committing an offence referred to in Art. 334 CPA, for interception, gathering and recording of electronic data (Art. 332(1), (2) CPA).

Directive 2014/41/EU regarding the European Investigation Order has been properly implemented in the Croatian legal system with the amendments to the Act on judicial co-operation in criminal matters with Member States of the European Union (JCCEU), which entered into force on 4 November 2017. The amendments to the JCCEU fully implemented Arts. 30 and 31 of Directive 2014/41/EU by prescribing it in an appropriate way in Art. 42.al and 42.am JCCEU.

1. International conventions

Croatia ratified the European Convention on Mutual Assistance in Criminal Matters on 5 March 1999 by the Law on ratification of European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 17 March 1978. Also, on the 15 December 2006, Croatia ratified the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 8 November 2001. Croatia ratified the Convention on Cybercrime on 3 July 2002 by the Law on ratification the Convention on Cybercrime of 23 November 2001. Croatia ratified the United Nations Transnational Organized Crime Convention on 7 November 2002 by the Law on ratification of the United Nations Transnational Organized Crime Convention of 15 November 2000.

2. Bilateral treaties

Most of the bilateral treaties that are in force in the Republic of Croatia and are used for mutual legal assistance date back to the time when Croatia was part of the Socialist Federal Republic of Yugoslavia. Yugoslavia signed two bilateral treaties on mutual legal assistance with Germany. First, the Agreement on Legal Assistance in Criminal Matters signed on 1 October 1971 entered into force on 8 January 1975; second, the Agreement on extradition of 26 November 1970 entered into force on 14 November 1975. Similar agreements have been signed with other EU countries like France, Bulgaria, the Netherlands etc. Following international recognition, the Republic of Croatia as one of the successors of the Socialist Federal Republic of Yugoslavia established the succession of bilateral agreements on the principle of "general succession," by exchanging notes or establishing diplomatic relations with those states. The notable feature of all the mentioned agreements is the fact that there are no specific provisions regarding the interception of electronic communications. Therefore, when it comes to providing legal aid based on a bilateral agreement then the CPA is applied as a rule. In the case of judicial cooperation between the EU Member States, the CPA will be applied as well as the JCCEU which implemented the EU Directive on the European Investigation Order in the Croatian legal system. Prior to the existence of the European Investigation Order, these bilateral agreements were the first choice in seeking mutual legal assistance, as they were given priority under the 1959 Convention. With the introduction of the European Investigation Order, their use for those countries applying the European Investigation Order ceased to exist.

3. National regulation

All legal assistance in Croatia is treaty/law-based. If the Republic of Croatia does not have a bilateral agreement or multilateral convention regulating international legal assistance, and there is a diplomatic relationship, the international legal assistance will be requested on the basis of the principle of reciprocity. This means that a country seeking international legal assistance must be prepared for the state from which it is seeking assistance to provide a guarantee that it will in future carry out a comparable request from a domestic judicial authority. Such a form of extrajudicial provision of international legal aid is governed by Art. 17 paragraph 1 of the Law on International Legal Assistance in Criminal Matters.

National regulation on interception of electronic communications is entirely regulated in the CPA. Therefore, the CPA regulates electronic interception with Arts. 332, 333, 335, 337 and 338 (see Annex VI).

B. Requirements and Procedure (Including the Handling of Privileged Information)

1. Incoming requests

Art. 42a of the Croatian Act on judicial co-operation in criminal matters with Member States of the European Union (JCCEU) stipulates:

> (1) Upon obtaining the decision of the judge of investigation, the competent county state attorney may, in accordance with domestic law, issue a European investigative order for the interception of computer data, surveillance and technical recording of telephone conversations and other telecommunications at a distance and verification of the establishment of telecommunications contacts in a Member State of which needs to be provided with technical assistance.
>
> (2) Where more than one Member State is in a position to provide the necessary technical assistance for the same interception of telecommunications, the European Investigation Order shall be addressed only to one of them. The advantage is always given to the Member State in which the interception entity is located or will be located.

Therefore, the telecommunications interception request is received by the Prosecutor's office (state attorney), which asks the judge to allow this measure. The Investigation Judge, in coordination with the Croatian State Attorney's Office, delivers their decision to the police, who "de facto" intercept communications by using the necessary technical equipment.

According to Arts. 10(1) and 12(1.3) of the Law on International Legal Assistance in Criminal Matters, there is a duty to filter out, or delete privileged information in the situation where the obtained data could represent a threat to public order. This obligation is also valid for real-time data to be transferred, but it would depend on the technical manner in which the measure is being implemented.

Additionally, the law in Croatia provides for the possibility to make the transfer of the intercepted data subject to conditions or require assurances from the requesting state. For details see 5.1.3.

2. Outgoing requests

The authorities responsible for sending such requests are the competent state attorney's offices (prosecutor offices). The competent public prosecutor or a judge, if the public prosecutor fails, is obliged to filter out any evidence he considers unlawful from the case file. This is a general rule that also applies to data collected by interception of telecommunications. This data could be used only for proceedings against the individual for whom the request has been made. This is a general rule applicable also for intercepted communications. Therefore, such data can be kept only as archival material (Art. 337(3) CPA). It can serve as information for some future inquiries, but its acquisition in the context of these new inquiries must be repeated within these inquiries, while respecting the above-described general procedures for their acquisition.

3. Real-time transfer of communications data

There is currently no regulation that would allow "real time cooperation" in the field of interception measures. Therefore, implementation of real time cooperation would represent serious violations of the rights and freedoms of an individual (right to freedom, privacy, etc.). To combat such potential violations, they must be strictly regulated by law with clearly prescribed preconditions to initiate and conduct those measures, authorities empowered to implement it, time limits and mandatory judicial review of legality and proportionality for determination and maximum duration of interception measures. This is not yet the case in Croatia. In addition, any other "relativisation" of such measures that are justifiably called "special" would constitute a dangerous violation of the fundamental rights and freedoms of individuals taking into account the standards of protection of fundamental human rights and freedoms at the European and international level.

C. European Investigation Order

Since the legislator has not fundamentally changed the way in which cross-border interception of telecommunications is conducted if requested in the system of mutual legal assistance in comparison with domestic cases, no major change is expected to occur. This conclusion can be drawn from the fact that provisions of the JCCEU are complemented with the provisions of the CPA as the ground rules on how to conduct those special measures. The changes that can be expected generally relate to the advantages of the European Investigation Order in comparison with the previous Rogatory Letters.

D. Statistics

There are no statistics of the Croatian Ministry of Justice on the extent of MLA-requests for electronic telecommunications interception. However, before the EIO came into force – cutting the Ministry out of the process – there were no more than five incoming requests per year for electronic telecommunications interception. There were a similar number of requests by Croatia for electronic telecommunications interception from foreign countries. This number does not represent an official report, but informal gathering of data by the authors of this study.

Annex I

1. Legitimacy of data transfers between different security agencies

Act on Security-Intelligence System of the Republic of Croatia (ASIS)

Article 59

(1) Based on their international commitments, the security intelligence agencies may co-operate with foreign security, intelligence and other corresponding services, through the exchange of information, equipment, through jointly conducted activities from their respective scopes, and through education of employees.

(2) The establishment and the suspension of the cooperation with each foreign service are approved by the National Security Council on the basis of the recommendations of the directors of the security intelligence agencies and the previously obtained opinion of the Council for the Coordination of Security Intelligence Agencies.

Article 60

(1) Security intelligence agencies may communicate to the appropriate foreign services the information on the citizens of the Republic of Croatia if they have been provided with relevant data indicating that such person is a threat to the national security of the state to which data is supplied, or to values protected by the international law. The information will not be provided if that would be contrary to the interests of the Republic of Croatia or if the protection of the interests of the person concerned is of greater value.

(2) When the security intelligence agencies conduct security vetting requested by some foreign service or international organisation of a person seeking employment in state authorities of foreign states or in the bodies of international organisations, it shall be conducted upon the receipt of a written consent of the vetted person.

(3) The delivered data must be entered into the records. Such data shall be accompanied by a notice indicating that they may only be used for the purpose they were provided for, and that the security intelligence agency providing the data retains its right to request feedback on how the provided information has been used.

Annex II

2. Other (non-constitutional) legal safeguards

Criminal Code

Article 143 Unauthorised audio recording and eavesdropping

(1) Whoever audio records without authorisation another person's privately uttered words or by means of special devices eavesdrops without authorisation another person's privately uttered words that are not intended to be heard by him/her

shall be sentenced to imprisonment for a term of up to three years.

(2) The sentence referred to in paragraph 1 of this Article shall be imposed on whoever uses or makes available to a third party the recorded words referred to in paragraph 1 or whoever publicly reveals word for word the eavesdropped words referred to in paragraph 1 or their gist.

(3) If the criminal offences referred to in paragraphs 1 and 2 of this Article are committed by a public official in the performance of his/her functions or the exercise of public authority,

he/she shall be sentenced to imprisonment for a term of between six months and five years.

(4) There shall be no criminal offence if the acts referred to in paragraphs 1 and 2 of this Article are committed in the public interest or another interest prevailing over the interest to protect the privacy of the person being recorded or eavesdropped on.

(5) The criminal offences referred to in paragraphs 1 and 2 of this Article shall be prosecuted upon request.

(6) The recordings and special devices used for committing the criminal offence referred to in this Article shall be seized.

Article 146 Unauthorized use of personal data

(1) Whoever, in contravention of the conditions set out in the act, collects, processes or uses personal data of physical persons

shall be sentenced to imprisonment for a term of up to one year.

(2) Whoever, in contravention of the conditions set out in the act, transfers personal data outside of the Republic of Croatia for further processing, or makes them public or in some other way available to a third party, or whoever by the act referred to in paragraph 1 of this Article acquires significant pecuniary gain for himself/herself or another or causes considerable damage

shall be sentenced to imprisonment for a term of up to three years.

(3) The sentence referred to in paragraph 2 of this Article shall be imposed on whoever commits the offence referred to in paragraph 1 of this Article against a child or on whoever, in contravention of the conditions set out in the act, collects, processes or uses personal data of physical persons on the racial or ethnic origin, political views, religious or other beliefs, trade union membership, health or sex life or the personal data of physical persons on criminal or misdemeanour proceedings.

(4) If the criminal offences referred to in paragraphs 1 through 3 of this Article is committed by a public official in the exercise of his/her authorities,

he/she shall be sentenced to imprisonment for a term of between six months and five years.

Article 269 Unauthorised interception of computer data

(1) Whoever intercepts or records without authorisation non-public transmissions of computer data, including electromagnetic emissions from a computer system, or makes available to another the data thus procured

shall be sentenced to imprisonment for a term of up to three years.

(2) A perpetrator who attempts to commit the criminal offence referred to in paragraph 1 of this Article shall be punished.

(3) The data derived from the commission of the criminal offence referred to in paragraph 1 of this Article shall be destroyed.

Annex III

3. Special protection of confidential communication content

Criminal Procedure Act (CPA)

Article 285

(1) The following persons are exempt from the duty to testify:

1) the defendant's spouse or common-law spouse,
2) the defendant's linear relatives by blood, collateral relatives by blood to the third degree and relatives by affinity to the second degree,
3) the defendant's adopted child and the defendant's adoptive parent,
4) notaries public, tax consultants within the scope of a legally binding confidentiality obligation,
5) attorneys, physicians, dentists, psychologists and social workers regarding information disclosed to them by the defendant while performing their respective professional duties,
6) journalists and their editors in the media, regarding sources of information and data coming to their knowledge in the performance of their profession and provided that their sources were used in the editorial process, except in criminal proceedings for offences against honour and reputation committed by the means of the media in a case prescribed by special law.

(2) Persons referred to in paragraph 1, items 4 to 6 of this Article cannot refuse to give a statement if a legal ground exists exempting them from their duty to keep information confidential.

(3) The authority conducting the proceedings is bound to remind the persons referred to in paragraph 1 of this Article that they are exempt from testifying before their examination, or as soon as the court finds out about their relation to the defendant. Persons referred to in paragraph 1, items 1 to 3, and shall be reminded that their testimony, if they nevertheless decide to give it, can be used as evidence, even if they change their decision later. The reminder and the answer shall be entered into the record.

(4) A child who, due to his/her age and mental development, is unable to understand the meaning of the right to exemption from testifying, cannot testify as a witness; however the information obtained from him/her through experts, relatives or other persons who have been in contact with him/her may be used as evidence.

(5) A person entitled to refuse to testify in respect of one of the defendants shall be exempted from the duty to testify in respect of other defendants as well, if his/her testimony cannot be, by the nature of the matter, limited only to other defendants.

(6) Persons referred to in paragraph 1, items 1 to 6 of this Article, except the defence counsel, and cannot refuse to testify in regard to criminal offences of criminal law protection of children.

.

Annex IV

4. Special protection of confidential communication content

Criminal Procedure Act (CPA)

Article 187

(1) Personal data may be collected by the competent authorities only for purposes specified by law in the framework of their tasks as laid down by the present Act.

(2) Personal data may be processed only in cases specifically provided for by statute or some other regulation and only to such extent as is in line with the purpose for which the data were collected. Further processing of the said data shall be permitted only if it is not incompatible with the purposes for which the data were collected and if the competent authorities are authorised to process such data for such other purpose in accordance with the law and such processing is necessary and proportionate to that other purpose.

(3) Processing of personal data concerning health or sex life shall be permitted only exceptionally if a criminal offence punishable by five years' imprisonment or a more severe penalty could not be detected or proven in any other way or where this would involve disproportionate difficulties.

(4) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership shall not be allowed.

(5) Personal data collected for the purpose of criminal proceedings may be transmitted to state administration bodies in accordance with a special act and to other legal persons only if the State Attorney's Office or the court determines that such data are required by them for a purpose laid down by law. Upon transmission, the said legal persons shall be warned that they have a duty to implement measures for the protection of data relating to the data subject.

(6) The personal data referred to in paragraph 1 of this Article may according to regulations be used in other criminal proceedings, in other proceedings for punishable acts in the Republic of Croatia, and in the framework of international legal assistance in criminal matters and international police co-operation.

Annex V

Regulation on national security requirements of the Republic of Croatia for individuals and legal entities in telecommunications (NSR), Articles 17 to 25

Data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

Data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

Data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

Data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

Data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

Annex VI

Criminal Procedure Act (CPA)

Article 332

(1) If the inquires of criminal offences cannot be carried out in any other way or would be accompanied by great difficulties, the judge of investigation may, upon the written request with a statement of reasons of the State attorney, order against the person against whom there are grounds for suspicion the he committed or has taken part in committing an offence referred to in Article 334 of this Act, measures which temporarily restrict certain constitutional rights of citizens as follows:

1) surveillance and interception of telephone conversations and other means of remote technical communication;

2) interception, gathering and recording of electronic data;

[…]

(4) Actions referred to in paragraph 1 item 1 of this Article may be ordered against persons against whom there are grounds for suspicion that that he delivers to the perpetrator or receives from the perpetrator of the offences referred to in Article 334 of this Act information and messages in relation to offences or that the perpetrator uses their telephone or other telecommunications devices, who hide the perpetrator of the criminal offence or help him from being discovered by hiding the means by which the criminal offence was committed, traces of the criminal offences or objects resulting or acquired through the criminal offence or in any other way.

[…]

(8) Under the conditions referred to in paragraph 1 of this Article, the measures referred to in paragraph 1 items 1, 2, 3, 4, 6, 7 and 8 of this Article may with his written consent be applied to means, premises and objects of that person.

Article 333

(1) Recordings, documents and objects obtained by the application of the measures referred to in Article 332 paragraph 1 item 1 to 8 of this Act may be used as evidence in criminal proceedings.

Article 335

(1) The order referred to in Article 332 paragraph 1 of this Act shall state the available data on the person against whom the measures are to be applied, the facts justifying the necessity for applying the measures and the term for their duration that should be proportionate to the accomplishment of the goal, as well as the manner, the scope and the place of execution of the measure. the measures shall be executed by the police authorities. Officials and responsible persons taking part in the decision-making process and execution of the measures referred to in Article 332 of this Act shall be bound to keep the confidentiality of the information that came to their knowledge in the process.

(2) The technical operation center for the supervision of telecommunications that carries out technical coordination with the provider of telecommunication services in the Republic of Croatia as well as providers of telecommunication services shall be bound to provide the necessary technical assistance to the police authorities. In case of proceeding contrary to this obligation, the judge of investigation shall upon the motion with a statement of reasons of the State Attorney impose a fine on a provider of telecommunication services in an

amount of up to HRK 1,000,000, and on a responsible person in the technical operative center for the supervision of telecommunications that carries out technical coordination and on a provider of telecommunication services in the Republic of Croatia in an amount of up to HRK 50,000, and if thereafter the ruling is not complied with, the responsible person may be punished by imprisonment until the ruling is executed, but not longer than one month. The panel shall decide on the appeal against the ruling on the fine and imprisonment. The appeal against the ruling on the fine and imprisonment shall not stay its execution.

(3) Special evidence collecting measures may last up to three months. Upon the motion of the State Attorney the judge of investigation shall, on account of important reasons, prolong the duration of such measures for a term of another three months. In specially complex cases (Article 334 (1) (2)), the judge of investigation may prolong the measures for a further term of six months. Exceptionally, for offenses referred to in Article 334 (1) of this Act, such actions may be extended for a further six months if their extension is necessary for gaining the purpose for which they have been approved. If judge of investigation denies the motion of the State Attorney to prolong the measures, the judge of investigation shall issue a ruling against which the State Attorney may file an appeal within eight hours. The panel shall decide on the appeal within twelve hours.

(4) As soon as the conditions referred to in Article 332 paragraph 1 of this Act cease to exist, the judge of investigation is bound to order the vacation of the measures undertaken. If the State Attorney desists from prosecution or if the data and information obtained by the application of the measures are not relevant for proceedings, they shall be destroyed under the supervision of the judge of investigation, who will draw up a separate record thereon.

(5) The order referred to in paragraph 1 of this Article shall be kept in a separate cover. After the termination of the measure and even before that, the order on measure may be delivered to the person the measure was ordered against if he so requests, provided that this is to the benefit of the proceedings.

(6) If in the course of the measures referred to in Article 332 paragraph 1 of this Act, data and information relating to another offence and perpetrator referred to in Article 334 of this Act are recorded, that part of the recording shall be copied and delivered to the State Attorney and may be used as evidence in the proceedings for that criminal offence.

(7) If the measures referred to in Article 332 of this Act are undertaken contrary to the provision of Article 332 of this Act, the evidence deriving from the data and information obtained in this manner may not be used as evidence in the criminal proceedings.

Article 337

(1) Measures referred to in Article 332 of this Act shall be carried out by the police authorities. The police authorities shall draw up daily reports on the process of execution and the documentation of the technical records, which they send to the State Attorney upon his request. The judge of investigation may at any time during the execution of special collection of evidence demand from a state attorney to submit to him a report on the course of such actions and the need for their further conduct. The judge of investigation may, when conducting special collection of evidence, request from the police, when necessary, the delivery of daily reports and technical documentation to assess the justification for their further implementation, to the extent determined by himself. If the actions are extended for six months in accordance with Article 335 (3) of this Law, the judge of investigation shall, after three months, request from the State Attorney submission of reports on the further need to carry out such actions.

(2) Upon the termination of the measure, the police authorities draw up a special report for the State Attorney's Office and the judge of investigation stating as follows: 1) time of the commencement and time of the termination of the measure; 2) number and identity of persons covered by the measure.

(3) The police authorities shall draw up the documents on technical recordings in two copies. One copy shall be kept in the police archive. The other copy enclosed with a special report shall be handed over by the police authorities to the State Attorney together with collected recordings and documentation.

[…]

(6) The application of measures referred to in Article 332 paragraph 1 of this Act shall cease as soon as the reasons lapse on the basis of which they were ordered. The State Attorney and the court shall by virtue of the office pay attention to the presence of the reasons on the basis of which the measures were ordered.

(7) The minister responsible for internal affairs, with a prior consent of the minister responsible for justice, shall bring regulations governing the method for conducting actions referred to in Article 332 of this Act.

Article 338

(1) Recordings, documents and objects obtained by carrying out the measures from Article 332 paragraph 1 of this Act may be used as evidence only in proceedings against the person referred to in Article 332 paragraph 1 of this Act.

(2) A complete recording, record and documentation shall be kept sealed in the State Attorney's office. When this is possible under circumstances, upon the motion of the State Attorney the investigating judge shall order that only those parts of the recording, record and documentation are excluded for the case file which refer to that criminal proceeding.

(3) For this purpose the State Attorney shall hand over to the judge of investigation a motion with a statement of reasons and a complete recording that the judge of investigation shall return after the exclusion of the part of the recording referring to that criminal procedure. The exclusion shall be conducted by an expert assistant under supervision of the judge of investigation.

(4) At the request of the defendant, the state attorney will immediately allow him to reproduce the record, or inspect the record or documentation. After the reproduction or insight into the record or documentation has been performed, the defendant may suggest that certain parts or complete footage, record or documentation be reproduced or read at the hearing.

List of Abbreviations

ASIS	Act on Security-Intelligence System of the Republic of Croatia
CJEU	Court of Justice of the European Union
CPA	Criminal Procedure Act
CTG	Counter Terrorist Group
ECA	Electronic Communications Act

ECHR	European Convention of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EIO	European Investigation Order
EUR	Euro
HRK	Croatian Kuna
JCCEU	Act on judicial co-operation in criminal matters with Member States of the European Union
MSIA	Military Security and Intelligence Agency
NSR	Regulation on national security requirements of the Republic of Croatia for individuals and legal entities in telecommunications
OTC	Operational Technology Centre for the Surveillance of Telecommunications
PDPA	Police Duties and Power Act
SIA	Security and Intelligence Agency
SOA	Security and Intelligence Agency
VSOA	Military Security and Intelligence Agency

Czech Republic

National Rapporteur:
Radim Polčák

Subordinate Rapporteurs:
Jakub Harašta,
Pavel Loutocký
Jakub Míšek
Václav Stupka

Revision as of fall 2018 made by:

Radim Polčák

Contents

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Security Services with Powers of Telecommunication Interception

1. National security architecture

One of the most important forming principles of the distribution of public powers in the Czech Republic is its totalitarian history. There is a strong distrust of official institutions in the general public. Thus, it can be seen that the procedures and powers of public bodies and agencies are set very rigidly. The principle of legality is set in Art. 2 para. 3 of the Czech Constitution (Act No. 1/1993 Sb., Constitution of the Czech Republic), which states that "State authority is to serve all citizens and may be asserted only in cases, within the bounds, and in the manner provided for by law"[1] and in Art. 2 para. 2 of the Charter of Fundamental Rights and Freedoms (Resolution of the Presidium of the Czech National Council of 16 December 1992 on the declaration of the Charter of Fundamental Rights and Freedoms as a part of the constitutional order of the Czech Republic No. 2/1993 Sb.), which states that "State authority may be asserted only in cases and within the bounds provided for by law and only in the manner prescribed by law."[2] Since all the public authorities authorized to conduct the interception of telecommunication fall within the scope of these articles, they are permitted to act only within the framework of what is expressly allowed to them by law.

In the Czech Republic, there are two regimes under which electronic communications can be intercepted. The first is the regime of criminal procedure conducted by police forces, including a special regime of customs service, and the second is a regime of civil and military intelligence services.

Act No. 141/1961 Sb. Code of Criminal Procedure, which sets the rules for the interception of communications in criminal proceedings, defines police authorities for its purpose in Section 12 para. 2 quite broadly (informal translation):[3]

Section 12 Code of Criminal Procedure

2) Police authorities mean

a) Bodies of the Police of the Czech Republic,

---

[1] English translation taken from the webpage of the Czech Constitutional Court. Online: http://www.usoud.cz/en/constitution-of-the-czech-republic/

[2] English translation taken from the webpage of the Czech Constitutional Court. Online: http://www.usoud.cz/en/charter-of-fundamental-rights-and-freedoms/

[3] English translation taken from the information system beck-online.

b) General Inspection of Security Forces in proceedings on criminal offences committed by members of the Police of the Czech Republic, members of the Prison Service of the Czech Republic, customs officers or employees of the Czech Republic classified to work in the Police of the Czech Republic, or on criminal offences by employees of the Czech Republic classified to work in the Prison Service of the Czech Republic or in the Customs Administration of the Czech Republic which were committed in connection with fulfilment of their employment duties,

c) appointed bodies of the Prison Service of the Czech Republic in proceedings on criminal offences of persons serving detention, a prison sentence or security detention that were committed in a custodial prison, prison or institute for the execution of security detention,

d) appointed customs authorities in proceedings on criminal offences committed by a breach of customs regulations or regulations on the import, export or transit of goods, even in cases of criminal offences by members of the armed forces or security forces, and by a breach of laws in the placement and purchase of goods in Member States of the European Communities if such goods are transported across the national borders of the Czech Republic, and in cases of tax infringements, where the customs authorities manage tax under special legal regulations,

e) appointed bodies of the Military Police in proceedings on criminal offences of members of the armed forces and persons who commit a criminal activity against members of the armed forces in military facilities, against military facilities, military material or other property of the State that is to be managed by the Ministry of Defence,

f) appointed authorities of the Security Information Service in proceedings on criminal offences committed by members of the Security Information Service,

g) appointed authorities of the Office for Foreign Relations and Information in proceedings on criminal offences committed by members of the Office for Foreign Relations and Information,

h) appointed authorities of Military Intelligence in proceedings on criminal offences committed by members of Military Intelligence,

i) appointed authorities of the General Inspection of Security Forces in proceedings on criminal offences committed by members of the General Inspection of Security Forces or on the criminal offences of employees of the Czech Republic classified to work in the General Inspection of Security Forces.

The police of the Czech Republic was established by Act No. 273/2008 Sb. on the police of the Czech Republic. Among its other duties, it is the main public authority for criminal investigation. It is organized on a geographical basis, as it is divided into divisions according to administrative regions. There are also several divisions with countrywide authority.[4] Of those, the most relevant Czech police divisions for this report are the National Antidrug Center,[5] Division for Uncovering

[4] In Czech: http://www.policie.cz/clanek/utvary-s-pusobnosti-na-celem-uzemi-cr-312510.aspx

[5] In Czech: www.policie.cz/narodni-protidrogova-centrala-skpv.aspx

of Corruption and Financial Criminality,[6] Division for Uncovering of Organised Crime,[7] and the Unit for Special Activities of Criminal Police and Investigation.[8]

The Czech police cannot use electronic communication interception as a preventive measure, since the law does not expressly allow it. This is due to the fact that Czech constitutional law strongly protects the privacy of an individual, and interception of communication is understood as a serious breach of such protection.[9] The law therefore quite rigidly formulates exceptions from this protection. Czech criminal procedure is governed by Act No. 141/1961 Sb. Code of Criminal Procedure. The interception of communication within the regime Code of Criminal Procedure can be undertaken only after the criminal proceedings have started. The preliminary hearing is the starting part of criminal proceedings in the Czech Republic and, as is stated in Section 158 Code of Criminal Procedure, it is commenced either by a criminal report submitted by a citizen or by the police authority itself as an *ex officio* act. It reads as follows (informal translation):

Section 158 Code of Criminal Procedure

(1) The Police Authority is obliged, based on their own findings, criminal reports, and instigations by other persons and authorities on the basis of which conclusions may be made on the suspicion of a criminal offence, to take all necessary investigations and measures to reveal the facts indicating that the criminal offence was committed and directed towards identifying the offender; they are obligated to take the necessary measures to prevent the criminal activity. The appointed authorities of the Prison Service of the Czech Republic shall inform the General Inspection of Security Forces without undue delay after they initiate such investigation.

(2) The public prosecutor and the police authority are required to accept reports of facts suggesting that the criminal offence was committed. At the same time, they are obligated to instruct the reporting person about the liability for knowingly false statements and if the reporting person requests it, to inform them on the effective measures taken within one month of the notification.[10]

Once the criminal proceedings have started and the legal prerequisites are met the police can commence with the interception.

A specific example of interception in accordance with the Code of Criminal Procedure is a regime of communication interception, which is grounded in Act

---

[6] In Czech: http://www.policie.cz/clanek/uokfk-skpv-utvar-odhalovani-korupce-a-financni-kriminality-skpv.aspx

[7] In Czech: http://www.policie.cz/clanek/vitam-vas-na-strankach-utvaru-pro-odhalovani-organizovaneho-zlocinu-570688.aspx

[8] In Czech: http://www.policie.cz/clanek/utvar-zvlastnich-cinnosti-sluzby-kriminalni-policie-a-vysetrovani-716842.aspx

[9] For example, the Czech Constitutional Court formulates the importance of this protection in Decision II. ÚS 502/2000 of 22 January 2001, which it followed up with Decision No. II. ÚS 615/06-1 of 23 May 2007, in which necessary conditions for allowing interception of communication were interpreted.

[10] Section 158, Act. No. 141/1961 Sb. Code of Criminal Procedure. In: ASPI [legal information system].

No. 17/2012 Sb. on customs service of the Czech Republic. Customs can, in certain cases, be considered a police force[11] and can act in accordance with rules for the criminal proceedings for obtaining authorisation to conduct the interception. Section 63 of Act No. 17/2012 specifies the cases over which the customs service has jurisdiction. The section states:

> **Section 63 Act on Customs Service – Basic Condition of Use**
>
> (1) Bodies of customs service may use operative search means, interception and recording of communication (thereinafter "operative search means") as set in the Code of Criminal Procedure, when fulfilling duties arising from international treaties during conducting of control of persons, about whom there exist serious reasons to suspect that they are breaching or have breached law of the second party to the treaty.
>
> (2) Rights and duties of bodies of customs service arising from the statutes regulating criminal procedure are not affected by conduct of control in the meaning of paragraph 1.
>
> (3) Operative search means may be used only in situation, when the breach of law of the second party to the treaty, would be considered in accordance with the Criminal Code[12] as an intentional crime, should it happen in the territory of the Czech Republic.[13]

As can be seen from the text, this can be understood as a preventive measure. The use of this provision is, however, strictly limited by the purpose of the interception, which is set out in para. 1 of the article:

> **Section 64 Act on Customs Service**
>
> (1) Usage of operative search means must not follow any other purpose than the one, which is specified in the concerned international treaty. Rights and freedoms of intercepted persons can be restrained on in the necessary manner.[14]

The Czech Republic has three intelligence services: The Office for Foreign Relations and Information (foreign intelligence service), Security Information Service (interior counter-intelligence service) and Military Intelligence. They are strictly separated from each other. This separation can again be interpreted as a result of Czech totalitarian history and general distrust of public institutions, especially those with executive power of this kind. *Lex generalis* covering these services is Act No. 153/1994 Sb. on intelligence services of the Czech Republic; the special acts are Act No. 154/1994 Sb. on the Security Information Service and Act No. 289/2005 on Military Intelligence. The rules for communication interception when conducted by intelligence services are included in these acts.

A specific case connected with intelligence services is the National Security Authority,[15] a body responsible for personnel and facility security clearance procedures. It has overall competences in the area of the protection of classified infor-

---

[11] See *supra* note 1.

[12] Act No. 40/2009 Sb., Penal Code.

[13] Section 63 of Act No. 17/2012 Sb. on customs service of the Czech Republic. In: beck-online [legal information system].

[14] Section 64 of Act No. 17/2012 Sb. on customs service of the Czech Republic. In: beck-online [legal information system].

[15] http://www.nbu.cz/en/

mation and, among other things, it issues personnel security clearance certificates. It is governed by Act No. 412/2005 Sb. on protection of secret information and security. Section 107 para. 3 of this Act, which covers personal security clearance procedures, empowers the National Security Authority to ask an intelligence service to carry out an examination of possible security risks in the environment of the candidate for clearance purposes:

Section 107 Act No. 412/2005

(3) In the proceedings on issuance of personnel security clearance certificates for the Top Secret degree the Office[16] shall conduct all the acts according to the paragraph 2 and furthermore it requests competent intelligence service to conduct an examination of possible security risks in the environment, in which the subject operates.[17]

This issue can be summed up as follows: There are two different and separate regimes of communication interception in the Czech Republic. Each of them has a different purpose and a different approval procedure (as can be seen in next question) and thus, generally speaking, data gained from one regime cannot be easily used in another.

2. Powers for the interception of telecommunication

a) Law of criminal procedure

Communication interception in the criminal procedure is established in Section 88 Code of Criminal Procedure. The relevant paragraphs on the procedure of authorisation of the interception are as follows:

Section 88 Code of Criminal Procedure – Interception and recording of telecommunications

(1) If criminal proceedings are conducted for a crime for which the law stipulates a prison sentence with the upper penalty limit of at least eight years, for a criminal offence of machinations in insolvency proceedings under Section 226 of the Penal Code, violation of regulations on rules of competition under Section 248 Subsection 1 Paragraph e) and Subsection 2 through 4 of the Penal Code, negotiating advantages during public procurement, tender and auction under Section 256 of the Penal Code, machinations during public procurement and tenders under Section 257 of the Penal Code, machinations at a public auction under Section 258 of the Penal Code, misuse of powers of an official person under Section 329 of the Penal Code or for any other intentional criminal offence for which prosecution is stipulated in a declared international treaty, an order for the interception and recording of telecommunications may be issued if it may be reasonably assumed that facts relevant to the criminal proceedings will be obtained in this way and if there is no other way to achieve such purpose or if its achievement would be otherwise significantly reduced. The Police of the Czech Republic perform the interception and recording of telecommunications for the needs of all law enforcement authorities. The interception and recording of telecommunications between the defence counsel and the accused is inadmissible. If the police authority finds during the interception and re-

---

[16] The National Security Authority.

[17] Section 107 para. 3 of Act No. 412/2005 Sb. on protection of secret information and security. In: beck-online [legal information system].

cording of telecommunications that the accused has communicated with their defence counsel, they are obliged to immediately destroy the interception recording and not to use the information learned in this context in any way. The report on the destruction of the record shall be placed in the file.

(2) The presiding judge and, in preliminary proceedings upon the petition of the public prosecutor, the judge, is entitled to warrant the interception and recording of telecommunications. If there is a criminal proceeding for an intentional criminal offence, the prosecution of which is governed by the applicable international treaty, the order for the interception and recording of telecommunications must be issued in writing and must be justified, including a specific reference to the applicable international treaty. The order for the interception and recording of the telecommunications service shall include a determined user address or a user device and the user if their identity is known, and the period during which the interception and recording of telecommunications traffic is conducted cannot be longer than four months; the justification must include the specific facts that justify the issue of such order as well as its period. The order for the interception and recording of telecommunications shall immediately be forwarded to the police authority. In the preliminary hearing, the judge shall send a copy of the order for the interception and recording of telecommunications to the public prosecutor without undue delay.

(5) The law enforcement authority may, without the order for the interception and recording of telecommunications, order the interception and recording of telecommunications or conduct it themselves if there is a criminal proceeding for the criminal offence of human trafficking (Section 168 of the Penal Code), the delegation of custody of a child to someone else (Section 169 of the Penal Code), restriction of personal freedoms (Section 171 of the Penal Code), extortion (Section 175 of the Penal Code), kidnapping of a child and persons suffering from a mental disorder (Section 200 of the Penal Code), violence against a group of people or an individual (Section 352 of the Penal Code), dangerous threats (Section 353 of the Penal Code) or dangerous persecution (Section 354 of the Penal Code), if the user of the intercepted unit agrees to such measure.[18]

The communication interception can be used for the sake of criminal proceedings only when the criminal proceedings are conducted for crimes specifically enumerated by the law. The general rule is that the interception must be initially authorized by a judge but, in certain cases, which are laid down in paragraph 5, prior consent of the person using the intercepted unit is sufficient.

The strict nature of this authorisation process was confirmed by the Czech Constitutional Court in Decision No. II. ÚS 615/06-1 of 23 May 2007. The court wrote the following in its decision:

"The right to protection of the secrecy of messages arising from Art. 13 of the Charter of Fundamental Rights and Freedoms, together with personal freedom and other constitutionally guaranteed fundamental rights, completes the personal sphere of an individual, whose individual integrity, as completely an essential condition for dignified existence and development of human life generally, must be respected and thoroughly protected as a token of respect for the rights and freedoms of man and citizen.[19]

If the constitutional order permits a breach of this protection, it does so solely and exclusively in the interests of a democratic society, or in the interest of the constitutionally

---

[18] Section 88 Code of Criminal Procedure. In: ASPI [legal information system].

[19] Paragraph 13 of the decision of the Czech Constitutional Court No. II. ÚS 615/06-1 from 23 May 2007. In: Codexis [legal information system].

guaranteed fundamental rights and freedoms of others. […] It is therefore permissible only such infringement of the fundamental rights and freedoms by the state power, which is necessary in this sense.[20]

It should be emphasized that an effective judicial review of the use of any operative means, with an overlap into the area of fundamental rights and freedoms, is absolutely crucial to a fair trial in criminal proceedings.[21]

In terms of the constitutional order is a violation of the secrecy of messages possible only in cases and manner prescribed by law. Statutory regulation interfering with this right must be formulated so that it does not deny this fundamental human right and thus it must also be interpreted. […] A court order for interception and recording of telecommunication operations must be written and reasoned. It must therefore be issued in respect to a person against whom criminal proceeding is conducted. If the proceedings is conducted on the basis of reasonable suspicion it must be explained in a recital what evidence support such conclusion. The mere criminal complaint itself, if it does not include explanation, is not sufficient for court order. […] The order may therefore be issued only in duly commenced criminal proceedings for legally qualified crime, and must be supported by relevant clues from which we can derive reasonable suspicion of committing such a crime. The order must be individualized in a relation to the specific person that is the user of intercepted telephone device. […] Finally, the order must at least at a minimal level specifically indicate what facts relevant for the proceeding are to be thus identified, and what is inferred from that."[22]

This strict approach was also acknowledged in Art. 67 Internal Order of the Police President No. 30/2009 of 21 April 2009 on the fulfilment of operations in criminal proceedings,[23] which was repealed by the Order of the Police President No. 103/2013 on the fulfilment of certain operations of the bodies of police of the Czech Republic in criminal proceedings.

Outside the regime of criminal procedure, the police can conduct communication interception when supervising a person who is protected in the special regime of witness protection. This is done in accordance with Section 10a of Act No. 137/2001 Sb. on special protection of a witness and other persons in connection with criminal proceedings. This interception can be commenced only after prior judicial authorisation:

Section 10a Permission to check on a protected person

(1) If there is given suspicion that the protected person fails to comply with the obligations specified in § 6, and is unable to verify this suspicion in another way, the Police is authorised, to the strictly necessary extent, to gain knowledge in a classified manner using technical or other means. The Police is authorised to make sound, visual or other records, conduct interception of communication and require on the person performing telecommunications services data on telecommunications traffic, which are the subject of telecommunications secrecy and subject to the protection of personal and agency data.

(2) Acquisition of audio, video or other recordings, interception and recording of telecommunications traffic and requesting data on telecommunications traffic is possible

---

[20] *Ibid*., paragraph 14.

[21] *Ibid*., paragraph 15.

[22] *Ibid*., paragraph 16.

[23] Available in Czech online: http://www.pecina.cz/files/pokyn2.pdf

only with the prior consent of the presiding judge of the High Court into whose jurisdiction belongs the seat of the police department or the prison service, which provides special protection and assistance. Against a decision to authorize or reject the application is not subject to appeal.[24]

The collection of traffic and location data by providers of electronic communications (data retention) and the possibility to access such data during the criminal proceedings by the police is laid down in Section 88a Code of Criminal Procedure:

Section 88a Code of Criminal Procedure

(1) If, for the purposes of criminal proceedings conducted for an intentional criminal offence for which the law sets out a prison sentence with an upper penalty limit of at least three years, for the criminal offence of violating the confidentiality of messages (Section 182 of the Penal Code), for the criminal offence of fraud (Section 209 of the Penal Code), for the criminal offence of unauthorised access to computer systems and information media (Section 230 of the Penal Code), for the criminal offence of procuring and possessing access devices and computer system passwords and other such data (Section 231 of the Penal Code), for the criminal offence of dangerous threats (Section 353 of the Penal Code), for the criminal offence of dangerous persecution (Section 354 of the Penal Code), for the criminal offence of spreading alarming news (Section 357 of the Penal Code), for the criminal offence of encouraging a criminal offence (Section 364 of the Penal Code), for the criminal offence of approving a criminal offence (Section 365 of the Penal Code) or for an intentional criminal offence for which prosecution is stipulated in a proclaimed international treaty binding on the Czech Republic, it is necessary to ascertain data on the telecommunications service that are the subject of a telecommunications secret or that are subject to the protection of personal and intermediation data, and there is no other way to achieve the pursued purpose or if its achievement would be otherwise significantly harder, their release to the public prosecutor or to the police authority shall be ordered by the presiding judge in proceedings before the court and by the judge upon the petition of the public prosecutor in a preliminary hearing. If there are criminal proceedings for a criminal offence the prosecution of which is stipulated in such international treaty, the order for ascertaining data on the telecommunications service must be issued in writing and must be justified, including a specific reference to the proclaimed international treaty. If the request applies to a particular user, their identity must be stated in the order, if known.

(2) The public prosecutor or the police authority by whose decision the matter was finally concluded, and in proceedings before the court the presiding judge of the court of first instance after the final conclusion of the matter, shall inform the user referred to in Subsection 1, if known, of the ordered ascertainment of data on the telecommunications service. The information shall identify the court which issued the order for the ascertainment of data on the telecommunications service, and detail the period to which such order applied. Such information shall include instructions on the right to submit to the Supreme Court, within six months of receipt of this information, a petition to review the legality of the order for the ascertainment of data on the telecommunications service. The presiding judge of the court of first instance shall submit the information without undue delay after the final conclusion of the matter, the public prosecutor by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the Attorney General under Section 174a, and the police authority by whose decision the matter was finally

[24] Section 10a of Act No. 137/2001 Sb. on special protection of a witness and other persons in connection with criminal proceedings and on change of Act No. 99/1963 Sb., Civil Procedure Code.

concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the public prosecutor under Section 174 Subsection 2 Paragraph e).

(3) The presiding judge, the public prosecutor or the police authority shall not submit the information under Subsection 2 in proceedings on a crime committed by an organised group for which the law stipulates a prison sentence with an upper penalty limit of at least eight years, in proceedings on a criminal offence committed for the benefit of an organised criminal group, in proceedings on the criminal offence of participation in an organised criminal group (Section 361 of the Penal Code), or if the commission of the criminal offence involved several persons and in relation to at least one of them criminal proceedings have not yet been finally concluded or if criminal proceedings are conducted against the person to whom the information is to be submitted, or if providing such information could defeat the purpose of the particular or some other criminal proceedings, or if it could threaten national security, life, health, or the rights or freedoms of individuals.

(4) An order under Subsection 1 is not required if the user of the telecommunications equipment to whom the data on the performed telecommunications service relates gives their approval for the provision of the information.[25]

In those cases, enumerated in paragraph 1, police can gain access to traffic and location data after preliminary judicial authorisation.

General authorisation for the Czech police to access location and traffic data is laid down in Section 66 para. 3 of Act No. 273/2008 on the Police of the Czech Republic:

Section 66 Police Act – Obtaining of information from records

(3) Police may, in cases prescribed by law and to the extent necessary to fulfill a specific task, request the legal or natural person providing a public communications network or publicly available electronic communications the traffic and location data in a manner, which enables remote and continuous access, unless another law provides otherwise. These persons are obliged to grant the request without undue delay, as and to the extent determined by other legislation.[26]

In three situations, however, the Czech police can access location and traffic data even outside the regime of criminal procedure.

The first situation concerns the search for persons and assets. This authorisation to access traffic and location data is established in the second paragraph of Section 68 of the Police Act.

Section 68 Police Act – Search for persons and assets

(2) Police can request legal or natural person providing a public communications network or publicly available electronic communications service traffic and location data in a manner enabling remote and continuous access, for a purpose of ongoing search for wanted or missing persons and for the purpose of identifying a person of unknown iden-

---

[25] Section 88a Code of Criminal Procedure. In: ASPI [legal information system].

[26] Act No. 273/2008 Sb. on the Police of the Czech Republic. In: beck-online [legal information system].

tity or the identity of the found corpse, unless another law provides otherwise. The information is provided in the form and to the extent determined by other legislation.[27]

Interestingly, location and traffic data can be accessed without prior judicial authorisation in this regime. This statement is also valid for the second situation, which is access to location and traffic data for the purpose of the fight against terrorism and preventing specific terroristic threats as laid down in Section 71 of the Police Act.

§ 71 Police Act

A police division, *competent in fight* against *terrorism*, *may for the purpose of preventing and detecting specific threats of terrorism to the extent necessary to request the*

a) legal or natural person providing a public communications network or publicly available electronic communications to provide traffic and location data in a manner enabling remote and continuous access, unless *another law provides otherwise*; *Information will be provided in the form and to the extent determined by other legislation.*[28]

The fact that location and traffic data can be accessed without prior judicial authorisation and the lack of other checks and balances[29] puts a strong tool in the hands of the police, which could be easily abused by the collection of a disproportional amount of data. This could in theory lead to a serious threat to personal data and privacy.

The last situation, in which the police can access traffic and location data outside the regime of criminal proceedings involves supervision over a person who is protected by the special regime of witness protection. Similar to communication interception, this permission is regulated by Section 10a of Act No. 137/2001 Sb. on special protection of a witness and other persons in connection with criminal proceedings.[30] In this case, prior judicial authorisation is necessary to access traffic and location data.

---

[27] *Ibid.*

[28] *Ibid.*

[29] Section 11 Police Act sets a general principle of proportionality; however, it is the opinion of the reporteur that this general provision is not sufficient reinsurance that the legal authorisation to collect such data will not be abused.

"Section 11 Adequacy of the procedure

A policeman and police employee are required to

ensure that no person suffered unwarranted injury due to their actions,

ensure that their decision not to act did not resulted in unsubstantiated harm to persons whose security is endangered,

proceed in a way that any possible interference with the rights and freedoms of persons to whom the act is directed, or any others, did not exceed what is necessary to achieve the objective pursued by the act."

Act No. 273/2008 on the Police of the Czech Republic. In: beck-online [legal information system].

[30] See *supra* note no. 24.

b) Preventive law

The Czech police cannot use electronic communication interception as a preventive measure, since the law does not expressly allow it.

c) Law of intelligence agencies

Generally speaking, the conditions which need to be met in order to legally carry out communication interception within the regime of intelligence agencies are less strict than those for interception in the criminal proceedings.

The wording of statutory authorisation to conduct communication interception in Acts No. 154/1994 Sb. on the Security Information Service and No. 289/2005 on Military Intelligence is practically identical. In both acts, the interception is grounded in Sections 8 and 9:

Section 8 – Intelligence technology

(1) Intelligence technology for the purposes of this Act means the technical facilities and equipment, especially electronic, photo-technical, chemical, physic-chemical, radio-optical, mechanical, or their files used in classified manner, if it causes interference with the fundamental rights and freedoms in

a) searching, opening, examining or evaluating transported consignments,
b) interception or recording of telecommunications, radio communication or other similar operation, or surveying data about this operation,
c) making video, audio or other records,
d) Search using technical means that could prevent or impede the fulfilment of operations within the scope of Military Intelligence/ Security Information Service,
e) identification of persons or objects, or to identify their movements using surveillance techniques and baits.

(2) Using intelligence technology, if it is not interfering with fundamental rights and freedoms, is not

a) capturing, listening, monitoring and evaluating information, which are distributed in a way that allows to access them by previously undefined group of persons
b) making video or audio recordings,
c) use security techniques and baits,
d) monitoring of telecommunications, radio communication or other similar operations without tapping its content, or collecting data on the traffic.

Section 9 – Application of intelligence technology

(1) Intelligence technology can be used by The Military Intelligence/the Security Information Service only when initially authorised by a written permission of the presiding judge of the High Court in whose jurisdiction falls the Ministry of Defence/the Security Information Service (hereinafter referred to as "judge"), under assumption that detecting and documenting of the activities for which is the technology to be used, would be ineffective or substantially more difficult or impossible, should it be done in a different way.

(2) Use of intelligence technology must not exceed the scope of the authorization of a judge under paragraph 1 and must not interfere with the rights and freedoms beyond what is strictly necessary.

(3) The Military Intelligence/the Security Information Service can technically secure the use of intelligence technology for the needs of other competent authorities, if they so request and submit appropriate authorization for the use of intelligence technology issued by a special legal regulation.

(4) The Military Intelligence/the Security Information Service is entitled to demand from the other for such activity authorized bodies the use of technical security intelligence technology for its own use. In this case, it is obliged to demonstrate that the use of intelligence technology has been authorised under provision this Act.

(5) Military Intelligence/the Security Information Service is entitled to the extent required for the performance of a specific operation, request a legal or natural person providing a public communications network or publicly available electronic communications service

a) the establishment or security interface for connecting the terminal telecommunications equipment for the interception or recording messages at specified points of their network, and

b) the provision of operational and localization data, in the form and to the extent determined by special legislation.[31]

The Office for Foreign Relations and Information is not expressly authorized by law to conduct communication interception. It is out of the scope of its competence, since the information collected by means of interception would be from within the borders of the Czech Republic. However, should the Office need to conduct such an interception, it can request it to be carried out by other intelligence services, most likely the Security Intelligence Service. This can be done on the basis of Section 9 of Act No. 153/1994 Sb. on intelligence services of the Czech Republic, which allows cooperation between services based on an agreement between them:

Section 9 Act No. 153/1994

Intelligence services cooperate with each other on the basis of agreements, which are concluded with the consent of the Government.[32]

Such interception would be completely within the legal regime of Act No. 154/1994 Sb. on the Security Information Service.

Even though the intelligence service needs judicial approval for the communication interception, just as it is needed in criminal proceedings, it is not limited to specific situations like the investigation of a crime enumerated in the statue. It is therefore legally easier to obtain such approval. This difference was elaborated by the Czech Constitutional Court in Decision No. I. ÚS 3038/07-1 from 29 February 2008 in which the Court stated that information obtained from the regime of intelligence service communication interception cannot be freely used in criminal pro-

---

[31] The provision marked here as paragraph 5 is marked as Section 8a in Act 154/1994 Sb. on security information service. Act No. 154/1994 Sb. on security information service and No. 289/2005 on military intelligence. In: beck-online [legal information system].

[32] Act No. 153/1994 Sb. on intelligence services of the Czech Republic. In: beck-online [legal information system].

ceedings.[33] Following a reminder of the Constitutional Court in this case, there is a difference in the purposes of the two regimes of communication interception. In the case of the criminal proceedings regime, the entire process is only within the judiciary branch of the state power, the purpose being solely the solving of crime; the evidence is obtained by the police based on the rules Code of Criminal Procedure and subject to a closer judicial review. In the case of the intelligence regime, it is rooted in the executive branch of state power, the purpose being national security; the judicial review is much less extensive than in the case of criminal proceedings. The court writes in paragraph 29: "Intelligence service interceptions do not reach the guarantee quality, which is required by the Code of Criminal Procedure and therefore they cannot be used in the criminal proceedings, because they were not obtained in the legal manner."[34]

In 2016, a legislative initiative aimed establishing a new agenda for the Military Intelligence in cyber-defence. The draft contained also the use "technical devices" that would be mounted onto major networks of electronic communications and would be, in theory, capable also of gathering data from respective networks. The draft did not contain any provisions making it legally possible for the devices to server to gather evidence for criminal proceedings. However, this initiative was abandoned after severe criticism raised during governmental and then parliamentary proceedings that pointed namely to the lack of safeguards of fundamental rights (namely privacy). Similar initiative was re-introduced at the time of editing of this report and it is, due to complex political situation in the Czech Republic, currently impossible to predict its further developent.

d) Financial and customs investigation service

As discussed above in I.A.1., the legal regime for communication interception specifically for the customs investigation service is stipulated in Section 63 of Act No. 17/2012 Sb. on customs service of the Czech Republic. This section, however, does not establish a new unique regime for message interception. It is only a specification of the criminal procedure regime, since the customs service may serve as a police force only in the first phase of the criminal proceedings, the preliminary hearing, and only in a situation described in the above-mentioned Section 63.

---

[33] In this case, the criminal proceedings against the defendant were commenced after the police obtained the military intelligence recording from the interception of the communication to which the defendant was a party. She was, however, not the legitimate subject of the interception. She issued a complaint against the commencing of the criminal proceedings, which was denied by the public prosecutor. After a series of appeals, the Constitutional Court ruled in her favour.

[34] Paragraph 29 of the decision of the Czech Constitutional Court No. I. ÚS 3038/07-1 from 29 February 2008. In: Codexis [legal information system].

Aside from the police and intelligence services, access to traffic and location data can be requested by the Czech National Bank. This can be done as a part of its responsibility to supervise the capital market, and prior judicial authorisation is required. However, the Czech National Bank is entitled to request the data from providers of electronic communications services directly, that means without use of police services:

Section 8

(1) The Czech National Bank is entitled for the purpose of performance of supervision over capital market to

a) request, after prior written authorisation by the presiding judge of the High Court under whose jurisdiction belongs the seat of the Czech National Bank, from a legal or natural person providing a public communications network or publicly available electronic communications traffic and location data in accordance to special legislation, if it can be reasonably assumed that data provided may contribute to the clarification of facts important for the detection of an administrative offense in the area of business or commerce in the capital market under the act governing capital market undertakings, including the offender, and if the pursued objective cannot be achieved differently, or if can be achieved only by exerting a disproportionate effort.[35]

3. Responsibility for the technical performance of interception measures

In the Czech Republic, the technical implementation of communication interception is done by the state agencies, with the cooperation of legaly bound subjects in accordance with Act No. 127/2005 Sb. on electronic communication. Section 97 para. 1 Act on Electronic Communications establishes a duty for the legal or natural person providing a public communications network[36] or publicly available electronic communications service[37] to provide and secure interfaces at specified points of the network for connection of terminal equipment for message tapping and recording. This is done at the requesting party's expense. This section authorizes the police of the Czech Republic, Security Information Service, and Military Intelligence to do so.

Access to traffic and location data is laid down in Section 97 para. 3 in a similar fashion. This provision authorises public authorities involved in the criminal proceedings, the police (for the sake of search for missing persons and assets and pre-

---

[35] Act No. 15/1998 Sb. on the supervision in the area of capital market and change and supplementation of some acts. In: beck-online [legal information system].

[36] Section 2 letter j) defines the public communication network as "an electronic communications network which is used wholly or mainly for the provision of publicly available electronic communications services and which supports transmission of information between end nodes of the network or an electronic communications network via which is provided service of television or radio broadcasting."

[37] Section 2 letter o) defines the publicly available electronic communications service as "electronic communications service from the use of which no person is excluded beforehand."

vention of terrorist activities), the intelligence services, and the Czech National Bank to request the legal or natural person providing a public communications network or publicly available electronic communications service to provide traffic and location data:

Section 97 Interface for communication interception and message recording

(1) Legal or natural person providing a public communications network or publicly available electronic communications service is required at the expense of the applicant to establish and ensure designated points on its network interface for connecting the terminal telecommunication equipment for wiretapping and recording information for

a) Police of the Czech Republic for the purposes established by special legislation,

b) Security Information Service for the purposes established by special legislation,

c) Military Intelligence for the purposes established by special legislation

(2) A legal entities or natural person providing public communications network or providing publicly accessible services of electronic communications is obliged to retain traffic and location data generated or processed within the provision of public telecommunications networks and provision of publicly available services of electronic communications […]. Legal entities and natural persons providing public communications networks or providing publicly available services of electronic communications are obliged to retain traffic and location data regarding unsuccessful call attempts solely under the circumstances when such data is generated and processed and simultaneously retained or recorded. Legal entities and natural persons retaining traffic and location data pursuant the first and the second sentences are obliged to immediately upon request provide such data to the bodies authorised to request such data as set forth by special regulations. Simultaneously such a person is obliged to ensure that the content of the messages and communications is not retained with the data described pursuant to the first and the second sentence. The period for which the data are retained must not be shorter than 6 months and longer than 12 months. Upon expiration of the above period the person retaining the data pursuant to the first and the second sentences is obliged to destroy the data should they have not been provided to the bodies authorised to request such data pursuant to special regulation or unless set forth otherwise by this Act. (Section 90).

(3) The extent of traffic and location data retained pursuant to para. 3, the period for which the data are retained pursuant to paragraph 3 and the form and manner in which they are to be submitted to the bodies authorised to use such data upon request pursuant to special regulation is to be set forth by a statutory instrument.[38]

When it comes to the criminal procedure regime of communication interception, the Unit for Special Activities[39] (a division with a countrywide authority) is the only division of the Czech police authorized to conduct the interception operations. A detailed procedure for this process is set out by the Order of the Police President No. 186/2011 upon request for tapping and recording of telecommunication traffic and upon request for traffic and location data, which was amended by the Order of the Police President No. 139/2012. This order is unfortunately not publicly accessible. However, the technical and request process is quite well described in the doc-

---

[38] Act No. 127/2005 Sb. on electronic communications and on amendment to some related laws (Act on Electronic Communications).

[39] Webpage of the division in Czech: http://www.policie.cz/clanek/utvar-zvlastnich-cinnosti-sluzby-kriminalni-policie-a-vysetrovani-716842.aspx

ument "Analysis of tapping and recording of telecommunication traffic," which was published by the Police Presidium of the Czech Republic on 6 June 2014.[40]

When the conditions of Section 88 para. 1 are met, the authorized person, who is the police investigator working on the criminal case, can request the interception. This request must contain a brief summary of the factual situation of the case and the reasoning for the request. It must especially contain anticipated facts, which are important for the case, and which should be uncovered during the interception. Furthermore, the request must include identification of the user unit that is to be intercepted (number, address, and name of its user, if known) and the period of time for which the interception should be conducted. This period may be no longer than four months. Before approval of the request, the designated officer of the Unit for Special Activities must be consulted; he/she will evaluate the request from a technical and operative point of view and decide whether the interception is possible and doable.[41]

If the criminal proceedings are in the preliminary hearing phase, the request is send to the Public Prosecutor, who then requests the interception from the court. In later phases of the proceedings, the court can be contacted directly. The court then issues a decision, namely a court order, which is delivered back to the Public Prosecutor (preliminary hearing) or directly back to the authorized person, who then delivers it to the Unit for Special Activities. When the conditions of Section 88 para. 1 are met, the authorized officer must obtain consent from the person using the intercepted unit. Once again, a properly filled out request is delivered to the Unit for Special Activities. In both situations, the division conducts the requested communication interception and the result of it, which is a sound recording recorded on a non-rewritable medium, is delivered back to the authorized person, who issued the request in the first place.

The court order must be specific and justified, including for example a reference to the specific international treaty, should the interception be conducted in the context of an intentional criminal offense for which prosecution is stipulated in a declared international treaty. The order must contain specific identification of the intercepted unit (address and identity of its user, if known) and the time period for which the interception is authorized.

After the end of the interception, the police body must in a short time evaluate the recordings and insert statistical data into the specialized system MU II. If the recordings are not to be used in the criminal proceedings, they must be destroyed three years after the proceeding has legally ended.

---

[40] In Czech online: www.mvcr.cz/soubor/ppr-102-31-cj-2014-990390-analyza-odposlechu-a-sledovani-za-rok-2013-pdf.aspx

[41] Analysis of tapping and recording of telecommunication traffic, p. 16.

If the recording of the telecommunication service is to be used as evidence, it is necessary to accompany it with a transcript, giving the place, time, manner, and contents of the record as well as the authority that issued the record. The police authority is obliged to label other records, securely store them so as to protect them against unauthorized misuse, and indicate the place of storage in the transcript. In another criminal case other than that for which the interception and recording of the telecommunication service was performed, the recording may be used as evidence if there is a criminal prosecution in this matter for a criminal offense referred to in para. 1 of Section 88 or with the consent of the user of the intercepted station or device:

Section 88 Code of Criminal Procedure

(6) If the record of the telecommunications service is to be used as evidence, it is necessary to accompany it with the transcript, giving the place, time, manner and contents of the record, as well as the authority which issued the record. The police authority is obliged to label other records, securely store them so as to protect them against unauthorised misuse, and indicate the place of storage in the transcript. In another criminal case other than the one in which the interception and recording of telecommunications service was performed, the recording may be used as evidence if there is a criminal prosecution in this matter for a criminal offence referred to in Subsection 1, or with the consent of the user by the intercepted station.

(7) If the interception and recording of the telecommunications service did not find any facts relevant to the criminal proceedings, the police authority, after approval by a court and in preliminary hearings, the public prosecutor, must immediately destroy all records after three years from the final conclusion of the matter. If the police authority was informed of an extraordinary appeal within the set deadline, they shall destroy the records of the interception after the decision on the extraordinary appeal or after a final conclusion on the matter. The police authority shall send a transcript on the destruction of the record of the interception to the public prosecutor, whose decision finally concluded the matter and in proceedings before the court, to the presiding judge in the first instance, for the record on file. [42]

The diagram at page 444 shows the request procedure for authorisation of communication interception.[43]

Section 19 of the Police Act of the Czech Republic authorizes the police forces to provide technical support and conduct communication interception for another public authority following a request and if that body is authorized to perform such action. The other public authority must declare this fact in its request:

Section 19 Police Act – Technical support

(1) The police can technically provide the use of intelligence technology or bait and security technology or a surveillance of persons and goods at the request of a public authority, which is authorised for such use.

(2) The public authority in the request demonstrates that the use of intelligence technology or surveillance of people and goods is authorised under special legal act.[44]

---

[42] Section 88 Code of Criminal Procedure. In: ASPI [legal information system].

[43] Analysis of tapping and recording of telecommunication traffic, p. 15.

[44] Section 19 Police Act. In: beck-online [legal information system].

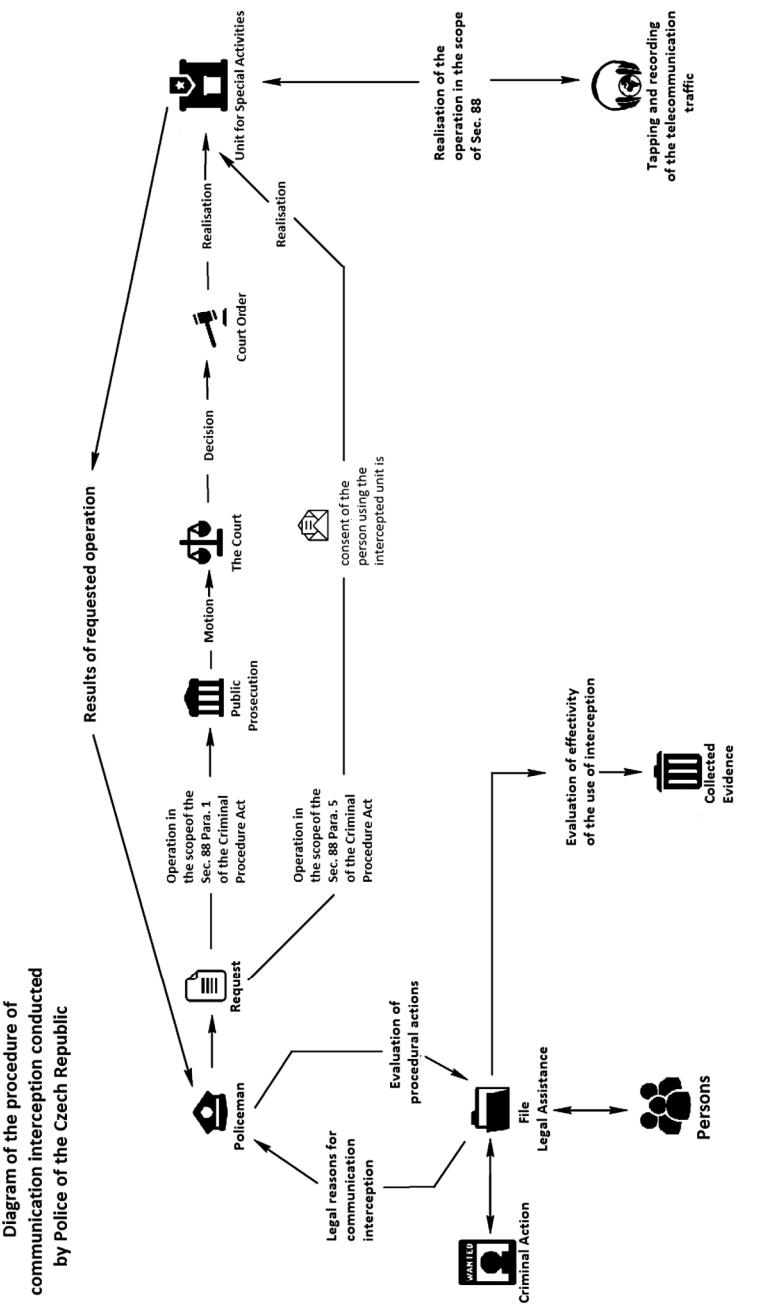


Diagram of the procedure of communication interception conducted by Police of the Czech Republic
Results of requested operation
Policeman
Request
Operation in the scopeof the Sec. 88 Para. 1 of the Criminal Procedure Act
Public Prosecution
Motion
The Court
Decision
Court Order
Realisation
Unit for Special Activities
Operation in the scopeof the Sec. 88 Para. 5 of the Criminal Procedure Act
consent of the person using the intercepted unit is
Realisation
Realisation of the operation in the scope of Sec. 88
Tapping and recording of the telecommunication traffic
Legal reasons for communication interception
Evaluation of procedural actions
File
Legal Assistance
Criminal Action
Evaluation of effectivity of the use of interception
Collected Evidence
Persons

This is the case for customs service since even though it is authorized by Section 63 of the Act on Customs Service of the Czech Republic to use communication interception, Act No. 127/2005 on electronic communications does not set a duty for electronic communications providers to allow customs service access to the networks. Customs therefore use services of the police (and therefore the Unit for Special Activities). However, the general directorate of customs is authorized to technically secure for other public authorities the application of intelligence techniques, including communication interception (Section 4 para. 5 letter c) of the Act on Customs Service). Similar to the above-mentioned Section 19 of Act No. 273/2005, this can be done upon request when the other public authority is authorized to perform such action:

Section 4 Act on Customs Service – Jurisdiction

(5) The General directorate of customs

c) in cooperation with public authorities secures, especially technically, the use of intelligence and security equipment or surveillance of persons and assets, if the relevant public authority proves that the it is authorized by law to conduct the interception.[45]

Interception of communication can be conducted by intelligence services within their specific legal regime. The rules for communication interception carried out by the Security Information Service and Military Intelligence are, as could be seen in above, almost identical. Both services can request the interception from the provider of public electronic communications and both can serve as technical support for other public bodies having authorisation to conduct communication interception (Section 9 paras. 4 and 5 of Act No. 289/2005 on Military Intelligence and Section 8a and Section 9 para. 4 of Act No. 154/1994 Sb. on the Security Information Service).[46]

The judicial authorisation procedure is the same for both intelligence agencies, and it is laid down in Section 10 of their respective acts (Act No. 289/2005 on Military Intelligence and Act No. 154/1994 Sb. on the Security Information Service):

Section 10 Authorisation to the use of intelligence technology

(1) The judge will issue the authorisation to the use of intelligence technology on the basis of written request, which includes

a) kind of intelligence technology, which is going to be used, period of time during which it is going to be used, basic identification data about the person (if known), against which the technology is going to be used, number of telephone or other similar station, should it be used for the communication interception, as well as the place of use of intelligence technology. Should the intelligence technology be used against member of government, member of Parliament or judge of the Constitutional court, or should the right to untouchability of household be breached, this information must be included in the request;

---

[45] Section 19 Act on Customs Service of the Czech Republic. In: beck-online [legal information system].

[46] See *supra*, question No. 2.

b) reasons for the use of intelligence technology;
c) information about any prior use of information technology against person indicated in the letter a) including the information, how was decided about that request.

(2) The judge will decide about the request without delay.

(3) The use of intelligence technology can be authorised only for the necessary period of time, at longest for 3 months. This period of time can be prolonged after a new request, but maximally only for 3 more months.

(4) The decision about authorisation to use of intelligence service includes kind of intelligence technology, which is going to be used, period of time during which it is going to be used, basic identification data about the person (if known), against which the technology is going to be used, number of telephone or other similar station, should it be used for the communication interception, as well as the place of use of intelligence technology.

(5) The judge issues along with the decision about authorisation to use of intelligence service also an abstract made from this decision, which includes the necessary identification data and statement, whether by use of intelligence service is breached the right to untouchability of household. The abstract does not include reasoning.

(6) Should the judge deny the request for authorisation to the use of intelligence technology, the decision must contain reasoning for such decision.

(7) Appellation against the decision is not allowed.[47]

An example of a public authority that can request the use of communication interception from the police and intelligence services is the General Inspection of Security Forces. According to Section 9 para. 2 a) of Act No. 341/2011 Sb. on the General Inspection of Security Forces, this authority can request communication interception of Security Forces and other public bodies to be conducted for the purpose of fulfilling its inspection duties. This interception is carried out within the legal regime of criminal procedure, since the request must include authorisation issued in the process governed by:

Section 9 Code of Criminal Procedure

(3) General Inspection may require from Security Forces and other public authorities, if it is necessary for the performance of a specific task of the Inspection

a) technical and personal resources for interception and recording of telecommunication operations or for operative intelligence means. In the request the Inspection demonstrates that the use of interception and recording of telecommunication operations or monitoring people and assets have been permitted under the Code of Criminal Procedure.[48]

The Chamber of Deputies of the Czech Parliament is the control body in regard to the communication interception for the police of the Czech Republic (Section 98 of Act No. 273/2008 Sb. on the Police of the Czech Republic) and the customs service (Section 65 of Act No. 17/2012 on the customs service of the Czech Republic). The Chamber of Deputies is also a control body for intelligence services in

[47] Act No. 154/1994 Sb. on Security Information Service and Act No. 289/2005 on Military Intelligence. In: beck-online [legal information system].

[48] Section 9 of Act No. 341/2011 Sb. on general inspection of security force. In: beck-online [legal information system].

general (Section 21 of the Military Intelligence Act and Section 18 of the Security Information Service Act); however, supervision of specific communication interceptions is done by courts (Section 11 of the Military Intelligence Act as well as of the Security Information Service Act).

General authorisation to request from electronic communications providers access to traffic and location data by the police of the Czech Republic is found in Section 66 para. 3 of Act No. 273/2008 on the Police of the Czech Republic. General authorisation to access such data by the intelligence services is found in Section 8a of Act No. 154/1994 Sb. on the Security Information Service and in Section 8 para. 5 of Act No. 289/2005 on Military Intelligence. Authorisation to access such data by the Czech National Bank is found in Section 8 of Act No. 15/1998 Sb. on supervision in the area of capital market and change and supplementation of some acts.

4. Legitimacy of data transfers between different security services

Generally speaking, the situation in the Czech Republic is similar to the situation in Germany because the regimes and functions are separate from one another. There are several reasons for this. The first one is the above-mentioned strong principle of legality. If the possibility of data transfer and sharing of information is not expressly written in the law, the agency cannot use the information collected by another agency. If the possibility of information transfer is written in the law it can be done only within the scope of the legal permission. The second reason for the separation is that different agencies intercept communications for different purposes and thus the process of obtaining permission for such interception also differs. Should the information be used in another regime than that for which they were collected, especially if interception conducted by the intelligence service is to be used in the criminal proceedings, it would be considered unlawful evidence and, as such, would not be admissible by the court. In paragraph 25 of the above-mentioned Decision No. I. ÚS 3038/07-1 from 29 February 2008,[49] the Czech Constitutional Court states that silence Code of Criminal Procedure about the possibility of using a communication interception obtained by a body other than the police, or not obtained in compliance with the Code of Criminal Procedure, as evidence in criminal proceedings needs to be interpreted in the light of the principle of legality, and therefore such interception cannot be used as an evidence.

a) Exchange of data between law enforcement authorities and preventive police authorities

As police authorities are not entitled to conduct communication interception for preventive purposes, and the interceptions for criminal proceedings are case-

[49] Paragraph 25 of the decision of the Czech Constitutional Court No. I. ÚS 3038/07-1 from 29 February 2008. In: Codexis [legal information system].

specific, this question is irrelevant for the Czech Republic as far as content data are concerned.

Data transfer is envisaged in Section 9 para. 3 of the Cybersecurity Act (Act No. 181/2014 Sb.) that reads as follows:

Section 9 Cybersecurity Act

(3) The Agency provides incidents record data to the public authorities for the purpose of fulfilling tasks within their authority.

This provision applies to data gathered by the National Cyber and Information Security Agency in the course of operation of the Governmental CERT[50]. These data include incident reports supplied by organisations that are obliged to report under the Cybersecurity Act (controllers of critical infrastructures and alike) and contain mostly traffic data and related information about handling of respective incidents[51]. In practice, these data are used only as an indication of a crime, but they regularly do not serve as evidence in court proceedings due to lack of their attributability to particular persons.

b) Passing on of data by intelligence agencies

A general authorisation for the intelligence services to pass on data is given in Section 8 para. 3 of Act No. 153/1994 Sb. on Intelligence Services of the Czech Republic:

Section 8 Act on Intelligence Services

(3) Intelligence services report to public and police authorities information about findings, which fall within their jurisdiction. *This does not apply if providing* of the information *threatens important interest pursued by the relevant intelligence service.*[52]

The intelligence service must provide information to other public bodies and police forces, findings which fall within their jurisdiction. It is not, however, permitted to pass on too much specific information, for that would be a violation of the principle of legality, as stated by the Czech Constitutional Court in paragraph 28 of the above-mentioned Decision No. I. ÚS 3038/07-1 from 29 February 2008.[53]

Passing on information within different intelligence services is not expressly covered by the law; therefore, it can only be carried out within the scope of the general provision.

---

[50] The Governmental CERT is regarded as the National CSIRT under the Art. 9 of the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

[51] For a detailed description of powers and functioning of the Governmental and the National CERTs, see *Polčák, R./Harašta, J./Stupka, V.*, Právní problémy kybernetické bezpečnosti. Brno : Masarykova univerzita, 2016.

[52] Section 8 of Act No. 153/1994 Sb. on Intelligence Services of the Czech Republic. In: beck-online [legal information system].

[53] *Ibid.*, paragraph 28.

c) Passing on of data to intelligence agencies

There are no specific provisions that expressly allow data to be passed from communication interception to intelligence services. However, there are authorisations for passing on information in general. This authorisation is not so specific and strong, so the principle of legality could be breached should it be used disproportionally.

For the police, the authorisation is laid down in Section 78 of Act No. 273/2008 Sb. on the Police of the Czech Republic. This section allows the police to hand over information, which was acquired during the fulfilling of their duties, to the national member of Eurojust, National Security Office, intelligence services of the Czech Republic, Military Police, Ministry of the Interior and other public bodies, should it be necessary for services in their jurisdiction:

Section 78 Police Act – Handover of information

(1) Police hands over information including the information processed in the police registers, which are gained during carrying out its tasks, to the national member of Eurojust, the National Security Office, the intelligence services of the Czech Republic, Military Police, the Ministry, the Prison Service of the Czech Republic, the Customs Administration of the Czech Republic and other public authorities, if it is necessary to perform the tasks within their scope.

(2) The Police does not pass the information if it would jeopardize the accomplishment of police tasks.[54]

Section 57 of Act on Customs Service of the Czech Republic (Act No. 17/2012 Sb.) contains very similar authorisation. This section authorizes customs services to pass on information to the same degree as does the above-mentioned Section 78 for the police:

Section 57 Act an Customs Service – Handover of information

(1) Customs authorities shall hand over information to

a) police,
b) intelligence services of the Czech Republic,
c) Military Police,
d) Ministry of Interior,
e) Prison Service of the Czech Republic,
f) the National Security Office, and
g) other public authorities, which in the area of competence of the customs administration are responsible for supervision or which conduct the proceedings on an administrative offense.

(2) Customs authorities hand over the information referred to in paragraph 1 only if the information is necessary for the performance of the legal tasks of these bodies.

(3) Customs authorities shall not transmit information when it would significantly jeopardize the performance of its duties.[55]

---

[54] Section 78 of Act No. 273/2008 Sb. on the Police of the Czech Republic. In: beck-online [legal information system].

The same scope also covers Section 37 of the Act on the General Inspection of Security Forces (Act No. 341/2011 Sb.), which authorizes General Inspection to pass on information to other public bodies:

Seciton 37 Act on the General Inspection of Security Forces

(1) Inspection hands over information, including personal data and information processed in the records of inspection, which are gained in carrying out its tasks to the Czech Republic Police, Prison Service of the Czech Republic, the Customs Administration of the Czech Republic, the Czech Republic's intelligence services, military police and other public authorities, if it is necessary to perform the tasks within their jurisdiction.

(2) The Inspection shall without undue delay hand over information which were collected during carrying out its tasks and which can be used in course of exempting a member of security forces from a service to the Director of the security forces; If this member is the director of a national security force, the inspection passes the information to his superior, Staff officers.

(3) Inspection of the information referred to in paragraphs 1 and 2 are not handed over, if it would undermine tasks of the Inspection.[56]

B. Statistics on Telecommunication Interception

1. Obligation to collect statistics

There is no statutory obligation to publish statistics on telecommunication interceptions. However, the police compiles statistics based on the order of the Police President No. 31/2012 on the analytical and statistical information system MU II.[57] This order is, unfortunately, not publicly available.

2. Current data

The Czech police annually publishes statistical reports on the use of electronic interceptions and the interception of persons and assets. The most recent one is the report from the year 2016.[58] These statistics include only communication interception, which was conducted within the regime of criminal proceedings under the provision of Section 88 Code of Criminal Procedure. Communication interception by intelligence services and customs in accordance with their special legal regimes

---

[55] Section 57 of Act No. 17/2012 Sb. on Customs Service of the Czech Republic. In: beck-online [legal information system].

[56] Section 37 of Act No. 341/2011 Sb. on General Inspection of Security Force. In: beck-online [legal information system].

[57] This order was issued upon a request of the Minister of Interior No. OBP-383-4/P-2007.

[58] In Czech online: http://www.mvcr.cz/soubor/analyza-odposlechu-a-sledovani-2016-pdf.aspx

is therefore not included in these statistics. Statistics on these kinds of communication interceptions are not publicly accessible.

The following data were taken from police statistics about absolute the number of interceptions, the number of intercepted stations and people and the differentiation of interceptions according to type of means used. Available statistics do not distinguish between interceptions conducted by different technologies, e.g., the detection of keystrokes, data tracking, etc. or whether they are telephonic interceptions.

	Total 2016	Regional Police Directorates	Police units with national jurisdiction
Total number of criminal files with intercepted communications	1617	1350	267
No. of criminal files where wiretapping[59] was authorised	1064	858	206
No. of criminal files where surveillance[60] was authorised	1084	867	217
No. of wiretapped telecommunication units	6717	4223	2494
No. of wiretapped persons	3802	2300	1502

The analysis also offers a chart with data concerning the effectivity of the perfomed interceptions. There are several categories that are used for this evaluation.

1) Active / Inactive interception

"Active" refers to interception that was commenced by the Unit for Special Activities of Criminal Police and Investigation and the information collected. Further categories (Nos. 2, 3, and 4) are subdivisions of this category.

There are two kinds of an "inactive" interception:

a) The Unit for Special Activities of Criminal Police obtained an authorized request for the interception, the interception was commenced and realized, but no recordings for the criminal procedure were obtained. An example of this situa-

[59] See Section 88 Code of Criminal Procedure.

[60] See Section 158d Code of Criminal Procedure.

tion is that the mobile telephone was inactive or the person of interest was not present in the Czech Republic.

b) The Unit for Special Activities of Criminal Police obtained an authorized request for the interception; however, the interception was not realized. For personal, technical, or other reasons no actions were taken by the Unit for Special Activities of Criminal Police for the entire time of validity of court authorization, and therefore no recordings were collected.

2) Direct influence on the criminal procedure

The collected information was, or will be, used:

a) as evidence in ongoing criminal proceedings;

b) for tactical reasons and further investigation;

c) to prevent another crime;

d) to capture a criminal offender.

3) Indirect influence on the criminal procedure

Collected information was, or will be, used for a discovery of:

a) a new criminal activity on the part of the criminal offender who was subjected to the interception;

b) a new criminal activity on the part of third persons who were not initially subjected to the ongoing interception.

4) Information obtained via the interception was not used

This category covers ineffective interception, because it did not lead to any information that could be used in the criminal procedure.

	Total	Regional Police Directorates	Police units with national jurisdiction
No. of intercepted telecommunication units	6717	4223	2494
Inactive interception	566	478	88
Direct influence on the criminal procedure only	4280	2390	1890
Indirect influence on the criminal procedure only	21	11	10
Combination of direct and indirect influence on the criminal procedure	978	816	162

Information obtained via the interception not used in criminal proceedings	872	528	344

The following statistics shows the development of numbers of authorized wiretappings over the last decade. There is apparent decrease between 2006 and 2009 and the increase between 2009 and 2014.

2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
7599	5491	4973	4571	5006	5766	6241	6689	7528	6978	6717

Another time-based chart demonstrates the development in average timeframe of authorized wiretapping (the figures show average length of conducted wiretapping in days).

2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
92,4	100,6	86,6	79,1	86,7	95,4	97,2	97,3	95,3	99,9	102,6

II. Principles of Telecommunication Interception in Constitutional Law and Criminal Procedure

A. Constitutional Safeguards of Telecommunication

1. Areas of constitutional protection

The Czech Republic also has, apart from the constitution itself, other documents that together form the Czech constitutional black-letter law – these are the constitutional laws and the Charter of Fundamental Rights and Freedoms. Together, these documents form the Czech Constitutional Order *(Ustavni poradek)*. Basic safeguards for the protection of fundamental rights are laid down in the Charter of Fundamental Rights and Freedoms that provides for their listing as well as brief explanations.

Recently applicable constitutional law (valid since 1993) already acknowledges privacy as a distinct distributive (individual) right. Apart from being mentioned in Art. 7(1) of the Charter of Fundamental Rights and Freedoms, it is also laid down specifically with regard to personal life in Art. 10(2), with regards to personal data in Art. 10(3), and with respect to communications and records in Art. 13.

Article 7(1) reads as follows (informal translation[61]):

> Inviolability of the person and of privacy is guaranteed. It may be limited only in cases specified by law.

Article 10(2) reads as follows (informal translation):

> Everybody is entitled to protection against unauthorized interference in his or her personal and family life.

Article 10(3) reads as follows (informal translation):

> Everybody is entitled to protection against unauthorized gathering, publication or other misuse of his or her personal data.

Article 13 reads as follows (informal translation):

> Nobody may violate secrecy of letters and other papers and records whether privately kept or sent by post or in another manner, except in cases and in a manner specified by law. Similar protection is extended to messages communicated by telephone, telegraph or other such facilities.

Privacy is laid down in the aforementioned provisions as a right *per se* (it does not form a subsequent right) that can be claimed individually. This means that privacy as a regulatory phenomenon consists of individualized protective rights that are all subject to judicial protection. This also means that whenever privacy is at stake, it should be possible to individually seek direct judicial protection or at least a judicial review of administrative decisions or other regulatory actions.

a) Secrecy of telecommunication

The secrecy of telecommunication is specifically recognized as a fundamental right in Art. 13 of the Charter of Fundamental Rights and Freedoms (see above). Legislation thereof is analogous to the traditional secrecy of letters, whereas any limitation of this protection has to be based on statutory law. This implies that telecommunication secrecy cannot be limited by bylaws or administrative decisions *per se* – any such limitation has to be grounded in the statutory law.

The fact that the secrecy of telecommunication is recognized by the Charter of Fundamental Rights and Freedoms as a distributive right implies that any infringement has to be reviewable by an independent judiciary. Together with the fact that telecommunication secrecy is a highly sensitive issue in the Czech Republic, this principle correspondingly led to currently applicable strict statutory safeguards for wiretapping.

---

[61] Resolution of the Praesidium of the Czech National Council No. 2/1993 Sb., English translation available at http://www.psp.cz/cgi-bin/eng/docs/laws/1993/2.html. For further citations, see *ibid*.

b) Confidentiality and integrity of information systems

There are no specific constitutional provisions regarding the confidentiality and integrity of information systems. Such protection, however, can be derived from more general fundamental rights. In this respect, it is to be noted that there is a reason to distinguish between the confidentiality and integrity of information systems as such and the confidentiality and integrity of data that are stored or communicated therein.

In the first case, specific protective tools are correspondingly based on the general protection of property laid down in Art. 11(1) that reads as follows: "Everybody has the right to own property. The ownership right of all owners has the same statutory content and enjoys the same protection, inheritance is guaranteed."

The latter case, i.e., the protection of data stored in information systems, is based on fundamental rights protecting specific types of information. Apart from the protection of privacy and personal data, these might include, e.g., the protection of trade secrets, protection of health records, protection of speech, etc.

The issue of confidentiality and the integrity of information systems is also closely linked to the active component of the concept of informational self-determination (see below). Recently, the protection of informational self-determination served as a constitutional basis for the adoption of the Cybersecurity Act,[62] which is primarily aimed at the establishment of security measures for protection of the confidentiality, security, and availability of critical information infrastructure.

c) Core area of privacy

The term "privacy" is used in Czech law to mean two things. One meaning is that it serves as a general constitutional principle, described above in II.A.1. Another meaning of the term "privacy" *(soukromi)* is primarily found in the Civil Code, and it establishes civil remedies for cases of infringement.

In Czech civil law, privacy protection is systematically put under the more general category of personality protection (apart from privacy, personality protection also includes the protection of dignity, esteem, etc.). The more general term "right to respect for private life" is regularly used when privacy is used as a regulatory principle that should limit powers or rights that lead to access to or processing of information originating in the private sphere of an individual (typically in personal data protection law, law on electronic communications, criminal procedure, etc.)

---

[62] Act No. 181/2014 Sb., English translation available at https://www.govcert.cz/download/nodeid-1143/

d) Right to informational self-determination

The German judicial concept of informational self-determination was adopted into Czech law through decisions of the Constitutional Court. It has recently been used in Czech constitutional practice as a common denominator for various individual information rights.

The Constitutional Court distinguishes between active and passive components of informational self-determination, whereas the passive component concerns various individual information rights that consist of the protection of information related to an individual from an unlawful interference. The active component of informational self-determination is based on the assumption that one cannot live a regular personal life without the ability to actively communicate (i.e., without the possibility to have an access to the means of communication that became established as a standard in the conventional interpersonal exchange of information).

The Constitutional Court used the active component of informational self-determination in a case in which a woman was sentenced for an economic crime, including subsequent damages.[63] In the trial, her petition for *pro bono* legal representation was refused based upon the fact that she regularly paid a relatively high fee for her cable TV and Internet connection at home (which was interpreted as a demonstration of the fact that she had sufficient funds to pay for her legal representation). The Constitutional Court held that requiring her to give up her Internet connection would mean a disproportionate limitation of her right to informational self-determination, one of the components of such right being the right to actively communicate. This decision of the Constitutional Court was partly criticized for its reasoning because the Court did not acknowledge the fact that the Internet connection might be obtained at significantly lower rates and that the active component of informational self-determination does not include a right to have an access to cable TV. However, the inclusion of the active component of informational self-determination had been accepted in Czech doctrine as one of possible forms of the interpretation of the right to personal life. The court held (official translation):

> The Constitutional Court also ascribed to this concept of the right to a private life, when it stated in its judgment file no. II. ÚS 517/99 that: "[T]he right to protection of personal privacy is the right of a natural person to decide according to his own deliberation whether, or to what extent and in what manner, the facts of his own personal privacy are to be made accessible to other subjects, and at the same time to defend oneself against (resist) unjustified interference in that sphere by other persons. Excessive emphasis on the positive component of the right to protection of one's private life leads to inappropriately narrowing of protection to merely seeing to it that the facts of a person's private life not be [disclosed] without his consent or without reasons recognized by the law, and thus the integrity of the internal sphere, which is essential for positive personal development, not be violated. The Constitutional Court does not share this narrowed under-

---

[63] Decision No. I. ÚS 22/10, English translation available online at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=372&cHash=1c2ede3ef55d98e9b6f7c2ebd4dc416b

> standing, because respect for private life must, to a certain degree, include the right to form and develop relationships with other human beings. Respect for private life, thus understood, includes the commitment of the state to act in a manner that permits the normal development of these relationships" [see judgment file no. II. ÚS 517/99 of 1 March 2000 (N 32/17 SbNU 229)].
>
> […]
>
> Therefore, it is the duty of the courts to review the unique aspects of each case so that, apart from observing the guarantees of a fair trial, the individual's other fundamental rights are also preserved, in this case the right to a private life [G. Dürig (G. D., Der Grundrechtssatz von der Menschenwürde, Archiv des öffentlichen Rechts 81, 1956, p. 127) formulated the well-known theory of the object, which was adopted in the case law of the German Constitutional Court, connected to questions of human dignity. According to this theory human dignity is violated when state authority places a particular individual into the role of an object, where he becomes a mere means, and is reduced to the form of a fungible value. One can conclude that a person not only the object of social "relationships," but also becomes the object of the law, if he is forced to subject to it completely in its interpretation and application, i.e. without taking into account his individual interests, or fundamental rights]. In addition to the subjective factors on the part of the individual, when evaluating whether expenses are "usual or justified" it is also necessary to take into account objective factors, which include, among other things, technological developments (e.g. mobile telephones, the internet) and related changes in methods of communication, obtaining information, contacts with government offices, association, etc., or the development of technologies, through which the individual's right to personal development, relationship with other people and the outside world, i.e. the right to a private life, is realized (point 17).

The active component of informational self-determination is to be distinguished from freedom of speech. Freedom of speech covers rights to actively communicate information to the public, i.e., the right to bring one's speech to the public space. In contrast, the active component of the right to informational self-determination (i.e., the right to communicate) includes only those forms of active communication that are common for individual private (personal) life, including private interpersonal communication, an individual requesting information (e.g., by browsing on a website), etc.

2. Proportionality of access to data

The doctrine of proportionality has constitutional origins, but it can now be seen as being applied by regular courts and even by administrative authorities. The methodological grounds for the proportionality of rights were established in a Decision of the Constitutional Court No. P. ÚS 4/94. In this case, the Court assessed the constitutional compliance of the institution of anonymous witness and had to find a proportional balance between witness protection and the fair trial rights of the accused.

With respect to a proportionate balancing of rights, the Court ruled that (official translation[64]):

> When considering the possibilities of restricting a basic right or freedom for the benefit of another basic right or freedom the following conditions can be stipulated governing the priority of one basic right or freedom:
>
> The first condition is their mutual comparison, the other is the requirement to examine the substance and the sense of the fundamental right or freedom being restricted (Art. 4 para. 4 of the Charter of Fundamental Rights and Freedoms[1]).
>
> The mutual comparison of colliding fundamental rights and freedoms is based upon the following criteria:
>
> The first is the criterion of applicability, i.e. a reply to the question whether the institute restricting a certain basic right allows the achievement of the desirable aim (the protection of another basic right). In the given case the legislator can be affirmed in that the institute of anonymous witness allows to achieve the aim, i.e. to guarantee the inviolability of his person.
>
> The second criterion for measuring basic rights and freedoms is the criterion of necessity residing in the comparison of the legislative means restricting some basic right or freedom with other provisions allowing to achieve the same objective, however, without impinging upon fundamental rights and freedoms. The reply to the fulfilment of the criterion of necessity in the second case is not unambiguous: in addition to the legislative construction allowing the anonymity of the witness the government can use also other means for his protection (such as the utilization of anonymous testimony as a criminalistic means for further examination, offering protection to the witness, etc.).
>
> The third criterion is the comparison of the importance of both conflicting basic rights. In the case under consideration one of them is the right of fair trial ensuring the right for personal freedom, the other is the right of personal inviolability. These basic rights are prima facie equal.
>
> The comparison of the importance of colliding basic rights (after having fulfilled the condition of appropriateness and necessity) resides in weighting empirical, systemic, contextual and value oriented arguments. As an empirical argument the factual seriousness of a phenomenon can be understood that is connected with the protection of certain fundamental right (in the case under consideration this is the increasing number of cases of threatening and terrorising of witnesses by organized crime). A systemic argument means considering the sense and the classification of the respective fundamental right or freedom within the system of basic rights and freedoms (the right to fair trial in this connection is part of the general institutional protection of basic rights and freedoms). As contextual argument also further adverse impacts of the restriction of one fundamental right due to the favouring another right can be understood (in the given case the possibility of misusing the institute of anonymous witness in the criminal procedure). The value argument represents considering the positive aspects of the conflicting fundamental rights as regards the accepted hierarchy of values.
>
> Part of comparing the relative weight of the conflicting basic rights is also considering the utilization of legal institutes minimizing the intervention into one of them, supported by arguments.

---

[64] Decision No. Pl. ÚS 4/94, English translation available at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=611&cHash=f69da5fcba1a2e433d74385371b3a196

As a result, the Court established a three-step test that consists of the following parts:

– suitability – whether the respective limitation of fundamental right(s) is able to serve the desired purpose;
– necessity – whether there might not be some other alternative ways to achieve the desired effect without the need to limit respective fundamental right(s);
– proportionality *stricto sensu* – whether there is a reason to prefer *ad hoc* one fundamental right over another.

If some limitation of a fundamental right is able to pass the above test, the additional need arises to assess whether the respective fundamental right will be limited only to a necessary extent. This assessment, also known as the limited proportionality test, is in many cases crucial. In the above-cited case of anonymous witness as well as in the case of data retention, the respective instruments went through all three tests. This means that the Court stated that these measures were fit for the purpose, there we no reasonable alternatives, and there was a reason to prefer certain fundamental rights over others. However, the Court held that the way in which these instruments were legislated into statutory law leads to a greater than necessary impact on respective fundamental rights. In other words, the Constitutional Court regularly holds that an instrument is proportionate *per se*, but it needs to be legislated using less intrusive measures or implementing more safeguards/balances.

The Czech doctrine of proportionality is to a large extent inspired by German constitutional practice as well as by the teachings of German legal scholars. Consequently, fundamental rights are all methodologically treated as legal principles, which means that none of them is *per se* superior to the other (their mutual relations have to be always resolved *ad hoc* in case of their collision). Thus, it is impossible to state, e.g., that privacy is generally more relevant than freedom of speech – on the contrary, every conflict of fundamental rights (or, in general, constitutional principles) has to be assessed on a case-by-case basis.

a) Implications for invasions of the secrecy of telecommunication

The doctrine of proportionality has been used in a number of cases, namely with regard to wiretapping. In most cases, the courts (the Supreme Court and the Constitutional Court) did not assess the mere question of *whether* wiretapping is compliant with a proportionate understanding of constitutional rights, but it also reviewed only *how* wiretapping was used in a particular case, including its procedural aspects. This means that in the Czech judicial practice wiretapping is not normally subject to review as to its mere existence but rather as to the form in which it is used in specific cases.

One specific issue in a number of cases also considered by the Constitutional Court was in the transferability of wiretapped records. In this respect, the Court had

to deal with subjective and substantive transfers. Substantive transfers are those that occur when, e.g., the police receive a court order for wiretapping based on a specific suspicion of a crime and it later turns out that it might be used as an evidence in a different criminal matter (e.g., the court order is obtained for the suspicion of fraud and it turns out later that wiretapped data can be used as crucial evidence in a case of blackmail). In these cases, the Constitutional Court has regularly ruled in favour of such use of wiretapped data.

In contrast, subjective transfers are those that take place not just based upon different causes but between different institutions. For instance, the domestic intelligence agency receives a court order for intelligence purposes and it turns out that the data can be used by the police in the investigation of a crime. In these cases, the Constitutional Court has regularly ruled against the admissibility of such evidence in criminal trials. However, it did rule that once the eventuality of possible use of wiretapped data by a different institution arises, such institution is obliged to request a new order.

b) Implications for access to traffic data

In terms of protection of fundamental rights against state intrusions, the Czech Republic is substantially different from countries that did not suffer from the Nazi or Communist rule. Even 25 years after political changes in 1989, the general social assumption about the normal functioning of the state and its security institutions is *a priori* negative. Even the Supreme Administrative Court and the Constitutional Court present themselves as judicial bodies whose main purpose is to protect an individual against intrusions committed by the state. Consequently, there is significant level of suspicion about any new forms of state activity that intrude on individual constitutional rights.

Unlike some other EU Member States, the Czech Republic had data retention legislated prior to the adoption of the Directive. Upon its adoption, the provisions laid down in the Telecommunications Act were broadened as was also the range of state institutions entitled to ask for this data.

The recently applicable version of data retention legislation is valid after the Constitutional Court had ruled against its first implementation. Using the doctrine of proportionality, the Court stated that the retention as such might be suitable to fulfil all three steps of the proportionality test, but that it does not meet the requirement of minimum possible intrusion (see *supra* II.A.2.).

The Court ruled that (official translation):[65]

> The primary function of the right of respecting private life is to provide space for development and self-realization of the individual personality. Apart from the traditional definition of privacy in its space dimension (protection of the home in a broader sense) and, in connection with the autonomous existence and public authority, undisturbed creation of social relationships (in a marriage, family or society), the right to respecting private life also includes the guarantee of self-determination in the sense of primary decision-making of an individual about themselves. In other words, the right to privacy also guarantees the right of an individual to decide, at their own discretion, whether and to what extent, how and under what circumstances the facts and information concerning their personal privacy should be made accessible to other entities. This aspect of the right to privacy takes the form of the right to informational self-determination, expressly guaranteed in Article 10, para. 3 of the Charter.
>
> The right to informational self-determination is thus a necessary condition not only for free development and self-realization of an individual, but also for establishing free and democratic communication rules. Put it simply, under the circumstances of an omniscient and omnipresent state and public authority, the freedom of expression, the right of privacy and the right of the free choice of behaviour and acting become virtually non-existent and illusionary.
>
> Although the prescribed obligation to retain traffic and location data does not apply to the content of individual messages [see Article 1, para. 2 of the Directive 2006/24/EC of the European Parliament and Council of 15 March on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereafter only as the Data Retention Directive) and the contested provisions of Section 97, para. 3, sentence 4) of Law No. 127/2005 Sb. on Electronic Communications and Amendment of Some related Acts (Act on Electronic Communications) in their latest wording] the data on the users, addresses, precise time, dates, places, and forms of telecommunications connection, provided that monitoring takes place over an extended period of time and when combined together, allows compiling detailed information on social or political membership, as well as personal interests, inclinations or weaknesses of individual persons.
>
> On condition that the criminal law allows for exercising the public interest to prosecute criminal activity by means of robust tools the use of which results in serious limitations of the personal integrity and fundamental rights and freedoms of an individual, then when applied, constitutional law limits have to be respected.
>
> Restrictions imposed on personal integrity and individual privacy (i.e. breaching the respect towards them) may only be applied as an absolute exception, provided it is deemed necessary in a democratic society, unless it is possible to meet the purpose pursued by the public interest in any other way and if it is acceptable from the perspective of the legal existence and respecting effective and specific guarantees against arbitrariness. Essential presumptions of a due process require that the individual be provided with sufficient guarantees against the potential abuse of power by the public authorities.
>
> With respect to the seriousness and extent of the infringement of the right to privacy in the form of the right to informational self-determination (in the sense of Article 10, para. 3 and Article 13 of the Charter), represented by the use of the retained data, the legislature limited the possibility to use the retained data only for the purposes of criminal proceed-

---

[65] Decision No. Pl. ÚS 24/10, English translation available at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=c574142df486769e0b435954fead08c3

> ings prosecuting serious crime and only in the case that such an objective cannot be achieved using any other means. In fact, this is anticipated not only by the Data Retention Directive, referred to above, but also by the provisions of Section 88, para. 1 Code of Criminal Procedure, defining the conditions for enacting interception and records of telecommunications operation ("on condition that criminal proceedings related to serious crime have been initiated"), from which the afore-mentioned legal regulation included in the provisions of Section 88a Code of Criminal Procedure as a whole deviates without any due reason, providing for the legal regulation in obvious contradiction to the opinions of the Constitutional Court.
>
> As for the examined case of global and preventive collection and retention of data on electronic communications, the need to have such guarantees available is becoming even more important to the individual owing to the current enormous and fast-moving development and occurrence of new and more complex information technologies, systems and communication tools, which unavoidably results in the borders between private and public space being blurred to the benefit of the public sphere, since in the virtual environment of information technologies and electronic communications (in the so-called cyberspace), every single minute, especially owing to the development of the Internet and mobile communications, thousands or even millions of items of data and information are recorded, collected and virtually made accessible, interfering with the private (personality) sphere of the individual, yet if asked, they would probably be reluctant to knowingly let someone else in.

We could speculate that the original draft of the reasoning of this decision might have contained even stronger statements about the actual constitutional disproportionality of the instrument of data retention as such. The final version of the reasoning, however, includes these formulations only in the form of rhetoric questions and only as a part of its *obiter dictum*. The very strong standing of the Court against the form in which data retention had been previously legislated can be in any case seen in the fact that respective provisions of Czech statutory law were repealed with immediate effect (this caused significant problems for law enforcement and security authorities in the interval between publication of the decision and adoption of new legislation).

In addition to above-cited decision, the Constitutional Court also ruled against a provision that originally provided the opportunity to request traffic data for the purpose of criminal procedure. In this case, the Court basically stated that procedural safeguards when requesting of traffic data should analogically be as strong as those in the case of wiretapping. The Court ruled (official translation):[66]

> It may be summarised that although Section 88a Code of Criminal Procedure contains the complete legal regulation of the access of the bodies active in criminal proceedings to the telecommunication traffic data, this access is expressly conditioned only by stipulating that the relevant data may be identified exclusively for the purposes of clarification of the circumstances significant for the criminal proceedings. Although the assessment as to whether this condition has been met is granted to the presiding judge or the judge within the preliminary proceedings who decides on ordering such data, its very general and vague definition cannot be deemed sufficient, taking into account the absence of any further regulation concerning the subsequent disposal of the data, as well as

[66] Decision No. Pl. ÚS 24/11, English translation available at http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/decisions/pdf/Pl_US_24-11.pdf

> in view of the fact that disclosing the data in question represents, in relation to the affected users of electronic communications services, an interference with their fundamental right to privacy in the form of the right to informational self-determination pursuant to Art. 10, para. 3 and Art. 13 of the Charter and Art. 8 of the Convention. Above all, the legislature failed to reflect at all in the contested provision the requirement of the proportionality of interference with fundamental rights with respect to the pursued goal, since the access to the data in question is provided for, in essence, as a common means of collecting evidence for the purposes of criminal proceedings, conducted even for any criminal offence. In view of the seriousness of the relevant interference with the private sphere of the individual, this limitation will only stand the test provided that it meets the conditions arising from the proportionality principle. This means that the access of the bodies active in criminal proceedings to the telecommunications traffic data may only come into question on condition that the purpose of the criminal proceedings cannot be achieved in any other way, that the legal regulation contains sufficient guarantees preventing the use of such data for any other purposes than those assumed by law, and that the restriction of the individual's right to informational self-determination does not amount to an excessive interference with respect to the importance of specific societal relationships, interests or values that are subject to the criminal offence for which the corresponding criminal proceedings are conducted. The contested provision does not respect these limitations, while this deficiency may not be eliminated even by means of the stipulated judicial review. In their decision making on ordering disclosure of the relevant data, courts may grant protection to the right to informational self-determination with respect to the facts of a particular case, yet their case law cannot replace the absence of a sufficiently definite and legitimate legal regulation, which is, pursuant to Art. 4, para. 2 of the Charter, a condition for placing limitations upon fundamental rights and freedoms in general.

In comparison with the case of substantive statutory provisions laying down mere data retention obligations, the procedural constitutional disproportionalities were not considered equally problematic by the Constitutional Court, despite having been found unconstitutional. We could also speculate that the Court might have noted serious problems caused by the immediate effect of its prior decision on data retention. Consequently, Section 88a Code of Criminal Procedure was repealed with enough delay to enable the adoption of a constitutionally compliant alternative.

The Court also expressly stated that, although the statutory procedure was unconstitutional as such, it does not imply *per se* a lack of constitutional compliance (and subsequent inadmissibility of retained data as evidence) in individual criminal cases. Despite later attempts by several accused or sentenced individuals to challenge the admissibility of such evidence in their trials, the results were mostly in favour of actual admissibility. In this respect, we might state that the lack of proportionality of substantive and procedural statutory rules for data retention were, in practice, often remedied by the constitutionally compliant actions of respective police forces, state prosecutors, etc. In other words, the police or Public Prosecutor acted at a higher standard of protection of individual rights in certain cases compared to what was expressly demanded by the applicable law.

c) Implications for intrusion into information systems

For a relatively long time, Czech law did not include any instrument making it *per se* illegal to intrude on an information system. Criminal law as well as civil law or administrative law included specific provisions that made it possible to sanction destructive intrusions (e.g., those that led to the damage of these systems or revelations of data) or intrusions against certain types of systems (e.g., systems containing classified data). Yet, mere intrusion was not *per se* subject to any kind of legal sanctions.

From the beginning of 2010, the criminal law contains different provisions providing for criminal liability in cases of simple intrusions. Consequently, it is possible to prosecute an offender upon proving the mere fact of intrusion (i.e., without the need to prove actual damage). The respective provisions of the Act No. 40/2009 Sb. the Penal Code read as follows:

Section 182 Penal Code – Violating confidentiality of messages

(1) Whoever intentionally violates the confidentiality

a) of a closed letter or other document during the provision of postal services or transported by other transport services or transport facilities,

b) of data, text, voice, audio or video messages sent via electronic communications networks and attributable to an identified subscriber or user who receives the message, or

c) of non-public transmission of computer data into a computer system, from or within which, including electromagnetic radiation from a computer system, transferring such computer data, shall be punished by a prison sentence of up to two years or punishment by disqualification.

(2) Whoever with the intention to cause damage to another person or to procure an unauthorised benefit for themselves or another person

a) reveals the secret of which they learned from the document, telegram, telephone call or electronic transmission through a communications network, which was not intended for them, or

b) takes advantage of such secrets, shall be similarly punished.

(3) An offender shall be punished by a prison sentence of six months to three years or punishment by disqualification, if

a) they committed an act referred to in Subsection 1 or 2 as a member of an organised group,

b) they committed such an act out of reprehensible motives,

c) they caused substantial damage by committing such an act, or

d) they committed such an act with the intention of gaining a substantial benefit for themselves or someone else.

(4) An offender shall be punished by a prison sentence of one to five years or a monetary penalty, if

a) they committed an act referred to in Subsection 1 or 2 as an official person,

b) they caused large-scale damage by committing such an act, or

c) they committed such an act with the intention to procure another large-scale benefit for themselves or someone else.

(5) An employee of postal services, telecommunications services or computer system or anyone else engaged in communication activities who

a) commits an act referred to in Subsection 1 or 2,

b) intentionally allows another person to commit such an act, or

c) amends or suppresses the document contained in a postal consignment or transported by transport facilities or a report filed by non-public transmission of computer data, telephone, telegram, or in another similar manner, shall be punished by a prison sentence of one to five years, a monetary penalty or punishment by disqualification.

(6) An offender shall be punished by a prison sentence of three to ten years, if

a) they caused large-scale damage by committing an act referred to in Subsection 5, or

b) they committed such an act with the intention to procure another large-scale benefit for themselves or someone else.

Section 183 Penal Code – Breach of confidentiality of documents and other privately kept documents

(1) Whoever violates the confidentiality of documents or other documents, photographs, film or other recordings, computer data, or other documents kept privately by another person without authorisation, by publishing, making them available to third parties, or otherwise uses them, shall be punished by a prison sentence of up to one year, a punishment by disqualification, or forfeiture of items or other assets.

(2) An offender shall be punished by a prison sentence of up to two years, a punishment by disqualification, or forfeiture of items or other assets, if they committed an act referred to in Subsection 1 with the intention to procure material or other benefits for themselves or someone else, to cause damage to another person or other serious damage, or to jeopardise their social esteem.

(3) An offender shall be punished by a prison sentence of six months to five years or a monetary penalty, if

a) they committed an act referred to in Subsection 1 as a member of an organised group,

b) they committed such an act against another person for their actual or perceived race, ethnicity, nationality, political belief, religion, or because they are actually or allegedly non-religious,

c) they caused substantial damage by committing such an act, or

d) they committed such an act with the intention of gaining a substantial benefit for themselves or someone else.

(4) An offender shall be punished by a prison sentence of two to eight years, if

a) they caused large-scale damage by committing an act referred to in Subsection 1, or

b) they committed such an act with the intention to procure another large-scale benefit for themselves or someone else.

[…]

Section 230 Penal Code – Unauthorised access to computer systems and information media

(1) Whoever overcomes security measures and thus gains access to a computer system or part thereof without authorisation shall be punished by a prison sentence of up to one year, punishment by disqualification, or forfeiture of items or other assets.

(2) Any person who gains access to a computer system or information medium and

a) uses data stored in a computer system or information media without authorisation,

b) erases or otherwise destroys, damages, amends, suppresses, or corrupts the quality of data stored in a computer system or information media, or renders them unusable without authorisation,

c) forges or alters data stored in a computer system or information media so as to be considered authentic and according to them it was treated as if it was authentic data, notwithstanding the fact whether the data is directly readable and understandable, or

d) inserts data into a computer system or information media or performs any other intervention into the software or hardware of the computer or other technical data processing equipment without authorisation,

shall be punished by a prison sentence of up to two years, punishment by disqualification, or forfeiture of items or other assets.

(3) An offender shall be punished by a prison sentence of six months to three years, punishment by disqualification, or forfeiture of items or other assets, if they committed an act referred to in Subsection 1 or 2

a) with the intention to cause damage to another person or to obtain an unauthorised benefit for themselves or another person, or

b) with the intention to restrict the functionality of a computer system or other technical equipment for data processing without authorisation.

(4) An offender shall be punished by a prison sentence of one to five years or a monetary penalty, if

a) they committed an act referred to in Subsection 1 or 2 as a member of an organised group,

b) they caused substantial damage by committing such an act,

c) they caused substantial interference in the activities of the State Administration body, local government, court, or another public authority by committing such an act,

d) they procured a substantial benefit by committing such act for themselves or another person, or

e) they caused serious interference in the activity of a legal entity or natural person who is an entrepreneur by committing such an act.

(5) An offender shall be punished by a prison sentence of three to eight years, if ,

a) they caused large-scale damage by committing an act referred to in Subsection 1 or 2, or

b) they procured another large-scale benefit by committing such act for themselves or another person.

Section 231 Penal Code – Measures and possession of access devices and computer system passwords and other such data

(1) A person who intends to commit a criminal offence of violating confidentiality of messages under Section 182 Subsection 1 Paragraph b), c) or a criminal offence of unauthorised access to computer systems and information media under Section 230 Subsection 1, 2 produces, puts into circulation, imports, exports, transports, offers, provides, sells, or otherwise makes available, procures for themselves or another person or possesses

a) a device or its component, process, instrument or any other means, including a computer programme, designed or adapted for unauthorised access to electronic communications networks, a computer system or part thereof, or

b) a computer password, access code, data, process or any other similar means with which they are able to gain access to a computer system or part thereof,

shall be punished by a prison sentence of up to one year, forfeiture of items or other assets, or punishment by disqualification.

(2) An offender shall be punished by a prison sentence of up to three years, punishment by disqualification, or forfeiture of items or other assets, if

a) they committed an act referred to in Subsection 1 as a member of an organised group, or

b) they procured a substantial benefit by committing such act for themselves or another person.

(3) An offender shall be punished by a prison sentence of six months to five years if they procured another large-scale benefit for themselves or another person by committing an act referred to in Subsection 1.

Section 232 Penal Code – Damage to computer systems and information medium records and intervention into the computer equipment out of negligence

(1) A person who violates, out of gross negligence, an obligation arising from their employment, occupation, position or function or one imposed by law, or one that is contractually assumed, and

a) destroys, damages, alters or renders unusable the data stored in a computer system or information media, or

b) makes an intervention into the hardware or software of the computer or other technical data processing equipment,

and thus causes substantial damage to the stranger's property, shall be punished by a prison sentence of up to six months, punishment by disqualification, or forfeiture of items or other assets.

(2) An offender shall be punished by a prison sentence of up to two years, punishment by disqualification, or forfeiture of items or other assets if they caused large-scale damage by committing an act referred to in Subsection 1.

The last article cited above provides for criminal sanctions only in cases in which damage to data is proven. It is analogous to the aforementioned provision in the repealed Penal Code that originally served the purpose of protecting information systems against intrusions.

The inclusion of criminal sanctions for mere intrusion of information systems triggered a negative response mainly from computer scientists. There was even a popular petition against the adoption of new types of criminal conduct into the Penal Code motivated by fears that the freedom of scientific research would be jeopardized (as with security assignments, research and development in computer sciences namely includes possession and use of intrusive tools that hypothetically fall under the above-cited provisions). The Penal Code, however, includes an escape clause (termed "material corrective" in Czech criminal law doctrine) that makes it possible to prosecute only conduct that is socially harmful. This requirement is laid down together with the *ultima ratio* principle in Section 12 para. 2 that reads as follows (informal translation): "The criminal liability of an offender and the criminal consequences associated with it may only be applied in socially harmful cases where application of liability under another legal regulation is insufficient."

3. Consequences for the interception of telecommunication

Historically, intrusive measures as well as protective instruments were primarily focused on real-time communication and specifically on telecommunication (nowadays indicated as "electronic communications"). Consequently, apart from the above-cited Charter of Fundamental Rights and Freedoms, there is a set of more or less traditional black-letter rules that lay down in detail procedures for wiretapping and subsequent use of acquired data.

In contrast, Czech law does not have experience with stored communications, i.e., with data that, for some reason, are stored somewhere and could be also used as evidence or as security intelligence. The only examples of relatively detailed rules that are related to stored communications are those implemented for the retention of traffic data. In any case, there is still a lack of more detailed provisions for communications (data) stored on personal devices and those stored by providers of information society services apart from electronic communications service providers.

For example, acquisition and forensic analysis of mobile communication devices are subject to the same rules as the acquisition of any other tangible assets. Similarly, there are no specific rules for the police or other forces with investigative powers to request data that are stored, mostly with the consent of users, by providers of hosting services[67] that fall outside the licensing regulations for providers of services of electronic communication. This, of course, does not mean that the police or the Prosecution Service would be entirely disqualified from working with stored e-mails or files in clouds – in these cases, they just have to apply general rules originally made with an entirely different teleology. Apart from the lack of efficiency, redundant formalities, or sometimes even the lack of logical sense (in some areas, the police uses the terms related to stored tangible assets in order to obtain stored data), this situation might also lead to a higher risk of *ad hoc* disproportionate infringement of constitutional rights. In the view of the national rapporteur, it is just a matter of time when the courts will start ruling against the admissibility of evidence obtained from stored communications if the general procedural tools used to acquire it did not *de facto* provide for enough safeguards as to informational self-determination or other individual (distributive) information rights.

a) Protection of the secrecy of telecommunication

Apart from the Charter of Fundamental Rights and Freedoms (cited supra II.2.1.), the secrecy of telecommunication is protected by a number of statutory

---

[67] Art. 14 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce").

provisions. In particular, the Act on Electronic Communications contains the following specific provisions (informal translation[68]):

Section 87 Act on Electronic Communications

(1) The rights and obligations relating to personal data protection, not regulated in this Volume, shall be governed by a special legal regulation.

(2) For the purposes of this Volume, consent based on a special legal regulation shall also be understood to mean consent granted by electronic means, including, but not limited to, the completion of an electronic form on the Internet.

(3) Supervision over compliance with obligations while processing personal data according to this Act shall be provided by the Office for Personal Data Protection in accordance with a special legal regulation.

Section 88 Act on Electronic Communications – Securing the protection of personal, traffic and location data and the confidentiality of communications

(1) An undertaking providing a publicly available electronic communications service is obliged to:

a) take technical and organisational measures to safeguard the security of the service in respect of the protection of natural persons' personal information in accordance with a special legal regulation, protection of traffic and location data, and confidentiality of the communications of natural persons and legal entities in providing the service; if necessary, the provider concerned shall, upon written agreement, also cooperate with the undertaking providing the communications network to provide protection,

b) prepare internal technical and organisational regulations to provide data protection and communications confidentiality in accordance with Clause (a) above; secure data protection and communications confidentiality with respect to the existing technical capabilities and the costs needed to provide protection at a level adequate to the risks of compromising the protection,

c) inform the subscribers concerned about the specific risk of the disturbance of network security in relation to data protection in accordance with Clause (a) above, and if the risk is beyond the scope of the measures taken by the undertaking, it shall also inform the subscribers about all the possible ways of remedying the situation, including the costs associated therewith,

d) establish internal procedures for handling requests for access to users' personal data; at the request of the Office for Personal Data Protection, undertakings providing a publicly available electronic communications service shall provide it with information about these procedures, the number of applications received, the legal justification of such requests and their responses.

(2) An undertaking providing a publicly available electronic communications service shall submit to the Office, if the Office so requests, the regulations referred to in Subsection 1 (c). If the Office finds that those regulations are in contradiction with this Act, the Office shall immediately notify the undertaking to that effect and shall grant the undertaking a reasonable period of time to remove any deficiencies.

(3) The Office is entitled, having requested the submission of the regulations referred to in Subsection 1 (b), to inspect how the undertakings providing a publicly available electronic communications service comply with those regulations, with the exception of inspections of compliance with obligations relating to the protection of personal data.

---

[68] Act No. 127/2005 Sb., English translation available online at http://www.mpo.cz/dokument156553.html.

(4) In the event of a breach of protection of the personal data of a natural person, the undertaking providing a publicly available electronic communications service shall notify this fact to the Office for Personal Data Protection without undue delay. Such a notification shall contain a description of the consequences of the breach of protection and the technical protection measures the undertaking has adopted, or proposes adopting.

(5) In the event of a breach of protection of the personal data of a user pursuant to Subsection 4 might have a particularly serious impact on the privacy of a natural person, or if an undertaking providing a publicly available electronic communications service failed to take measures to remedy this situation and which would have been sufficient to protect the personal data at risk, in accordance with an assessment by the Office for Personal Data Protection, it shall also notify this fact to the individual concerned and to the Office for Personal Data Protection. In this notification, the undertaking shall indicate the nature of the breach of personal data protection, recommendations for the implementation of interventions to mitigate the impact of the breach of personal data protection and the contact information location.

(6) The Office for Personal Data Protection is entitled, after investigating the situation resulting from the breach of protection pursuant to Subsection 4 above, to impose an obligation on an undertaking providing a publicly available electronic communications service to inform the individual concerned of the breach of personal data protection, if it has not already done so.

(7) An undertaking providing a publicly available electronic communications service shall maintain, only for the purposes of reviewing compliance with obligations pursuant to Subsections 4 and 5, a list of breaches of personal data protection, including information on the circumstances of the breach, its impacts and measures adopted to remedy the situation. An implementing legal regulation may lay down more detailed conditions under which the undertaking providing a publicly available electronic communications service is required to notify any breach of personal data protection, the format of such a notification and the manner in which the notification is to be made.

Section 88a Act on Electronic Communications

(1) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service shall ensure that the traffic and location data stored in accordance with Section 97 Subsection 3 are of the same quality and subject to the same security and protection against unauthorised access, alteration, destruction, loss or theft or other unauthorised processing or use, as the information referred to in Section 88; this does not affect the obligations set out in a special legal regulation[34]).

(2) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service shall draft internal technical and organisational rules to ensure data protection in accordance with Subsection 1; it shall provide data protection with regard to the existing technical possibilities and to the costs required to provide protection at a level appropriate to the risk of breach of protection. The provisions of Section 88 Subsections 2 to 7 shall apply mutatis mutandis to data protection under this provision.

Section 89 Act on Electronic Communications – Confidentiality of communication

(1) Undertakings providing a public communications network or a publicly available electronic communications service shall implement technical and organisational measures to safeguard the confidentiality of the messages and the related traffic and location data, which are transmitted via their public communications network and the publicly available electronic communications services. In particular, such undertakings shall not admit any tapping, message storage, or any other types of interception or monitoring of

messages, including the data contained therein and related thereto, by any persons other than the users, without the consent of the users concerned, unless otherwise provided in an Act[36]). This shall not be to the prejudice of the technical storage of data as needed for message transmission without affecting the confidentiality principle.

(2) A message means any information being exchanged or transmitted between a finite number of subscribers or users via the publicly available electronic communications service, except for the information transmitted as part of the public radio or television broadcasting service via the electronic communications network, unless it can be allocated to an identifiable subscriber or user receiving that information.

(3) Anybody wishing to use, or using, the electronic communications network for the storage of data or for gaining access to the data stored in the subscribers' or users' terminal equipment shall inform those subscribers or users beforehand in a provable manner about the extent and purpose of processing such data and shall offer them the option to refuse such processing. This obligation does not apply to activities relating to technical storage or access and serving exclusively for the purposes of performing or facilitating message transmission via the electronic communications network, nor does it apply to cases where such technical storage or access activities are needed for the provision of an information society service explicitly requested by the subscriber or user.

Section 90 Act on Electronic Communications – Traffic data

(1) Traffic data mean any data processed for the purposes of the transmission of a message via the electronic communications network or for the billing thereof.

(2) An undertaking providing a public communications network or a publicly available electronic communications service who processes and stores traffic data, including the appropriate location data relating to a user or subscriber, shall erase such data, or render them anonymous, once they are no longer needed for message transmission, except as provided in Subsections 3 to 6. The obligation of the legal entity or natural person providing a public communications network or a publicly available electronic communications service to maintain traffic and location data in accordance with Section 97 shall remain unaffected.

(3) An undertaking providing a public communications network or publicly available electronic communications service shall store traffic data for services provided to a subscriber or user until such time as a dispute pursuant to Section 129 Subsection 3 has been resolved, or until the end of the period during which the prices may be billed or the provision of an electronic communications service may be legally challenged or settlement recovered.

(4) An undertaking providing a public communications network or a publicly available electronic communications service may process the traffic data essential for the billing of the service provided to a subscriber or user for access, to the end of the period during which payment may be recovered.

(5) Undertakings providing a public communications network or a publicly available electronic communications service may provide each other with data related to the provision of the service, including, but not limited to, data about the subscribers being connected, in order to ensure interconnection and access to the network, mutual billing, and identification of any abuse of the electronic communications network and services. Abuse of electronic communications networks and services means consistent late payment of bills in accordance with Section 64, or the making of malicious or annoying calls.

(6) For the purposes of marketing the electronic communications services, or for the provision of value-added services, the undertaking providing a publicly available electronic communications service may only process the data referred to in Subsection 1

above to the extend and for the period needed for such services or such marketing, provided the subscriber or user to whom the data relate have given their consent thereto. The subscriber or user may withdraw their consent to the processing of traffic data at any time.

(7) A value-added service means any service for which it is necessary to process traffic data – or location data other than traffic – beyond what is needed for the transmission of a message or for the billing thereof.

(8) The undertaking providing a publicly available communications service shall inform the concerned subscriber or user about the traffic data being processed and about the time for which such data may be processed for the purposes referred to in Subsections 3 to 5. For the purposes referred to in Subsection 6, the undertaking shall so inform the subscriber or user to whom the data apply before obtaining the consent of such a subscriber or user.

(9) An undertaking providing a public communications network and an undertaking providing a publicly available electronic communications service shall ensure that the traffic data processing, in accordance with Subsections 2 to 6 is restricted to:

a) the persons who were authorised to that effect by the undertaking and who are responsible for the billing or operations management, customer inquiries, fraud identification, electronic communications services marketing, or who provide value-added services, and
b) the extent essential for the activities referred to in Clause (a) above.

Section 91 Act on Electronic Communications – Location data

(1) Location data means any data that are processed within the electronic communications network and that define the geographical location of the terminal equipment of a user of a publicly available electronic communications service.

(2) If an undertaking providing a public communications network or publicly available electronic communications service performs the processing of location data other than traffic data, which have a bearing on a user or subscriber, such an undertaking shall render this data anonymous or obtain the user's or subscriber's consent to the processing of such data to the extent and for the period as needed for the provision of value-added services. Before gaining such consent, the undertaking shall inform the user or subscriber concerned about the type of location data to be processed other than traffic data, about the purpose and length of the processing and of whether the data are to be made available to a third party for the provision of value-added services. The user and subscriber may withdraw his/her consent to the data processing at any time.

(3) If the user or subscriber gave his/her consent to the processing of location data other than traffic data, the undertaking providing a public communications network or a publicly available electronic communications service shall offer the user or subscriber the operation of temporarily refusing the processing of the data in accordance with Subsection 2 above for every connection to the network of for every message transfer. Such an option shall be provided free of charge and only entail simple processes.

(4) An undertaking providing a public communications network, an undertaking providing a publicly available electronic communications service and an undertaking providing value-added services shall ensure that the data referred to in Subsections 2 and 3 are only processed by persons duly authorised and entitled to that effect by internal technical and organisational regulations within the meaning of Section 88 Subsection 1 (b); the processing must be restricted to the extent essential for the needs of such activities.

Section 92 Act on Electronic Communications – Display of incoming call number

(1) An undertaking providing a publicly available telephone service is obliged, in the event that the opportunity is offered, to display the subscriber number:

a) of the calling subscriber, to offer the calling subscriber the possibility free of charge to prevent the display of his/her subscriber number for each individual call, using simple means. The calling subscriber shall have this option for each subscriber number,

b) of the calling subscriber, to offer the called subscriber the possibility of preventing the display of the calling subscriber number for incoming calls, using simple means and providing this function free of charge in justified cases, such justified cases being, without limitation, workstations from which personal crisis situations are solved (for example hot line services),

c) of the calling subscriber, and displaying this number before the call is actually connected, to offer the called subscriber the possibility of refusing the incoming calls, for which the calling subscriber restricted the display of his/her subscriber number, using simple means,

d) of the called subscriber, to offer the called subscriber the possibility of preventing the display of his/her subscriber number for the calling subscriber, using simple means and providing the service free of charge.

(2) The provisions of Subsection 1 (a) shall also apply to calls from the Member States of the European Union routed to third states. The provisions of Subsection 1 (b), (c) and (d) also apply to incoming calls from third states.

(3) Where display of the calling or called number is offered, the undertaking providing a publicly available electronic communications service shall inform the public of the possibilities referred to in Subsection 1 above.

(4) An undertaking providing a public communications network or a publicly available electronic communications service is entitled to cancel the barring of the display of the calling subscriber number:

a) temporarily, at the request of a subscriber, who has requested that a malicious or annoying call be traced; in such a case, the undertaking shall store and make accessible to the aggrieved subscriber information containing the calling subscriber identification, and

b) and continue to process the location data during the transmission of calls to every emergency call number operated by the relevant facility for the reception of such calls, even despite a temporary ban or the lack of consent from the subscriber concerned.

(5) An undertaking providing a public communications network or a publicly available electronic communications service shall make public in its commercial facilities, and in a manner allowing remote access, the mandatory procedures to be followed in order to impose the two options referred to in Subsection 4 above, and shall inform its subscribers to that effect.

Section 93 Act on Electronic Communications – Abuse of electronic mail addresses of the sender

It is prohibited to use any electronic mail address to send a message or messages to third parties without the consent of the holder of that electronic mail address.

Section 94 Act on Electronic Communications – Call forwarding

(1) Any undertaking providing a public communications network or a publicly available electronic communications service shall ensure, using simple means, that every sub-

scriber can enjoy, free of charge, the possibility of preventing automatic forwarding of calls by a third party to the subscriber's terminal equipment.

(2) In the event that, during the provision of the publicly available electronic communications service, calls are forwarded automatically or in a concealed manner to another service or to a service provided by another undertaking, or a new connection is established, thereby increasing the price to be charged, the person providing the publicly available electronic communications service shall notify the user of this fact free of charge and allow him/her to stop the call before it is forwarded or a new call is established. If calls are forwarded or a new connection is established and, as a result, the price to be charged is increased without notification of the user to that effect by the person providing a publicly available electronic communications service at the increased price, the Office shall decide to stop the provision of such service.

Section 95 Act on Electronic Communications – Subscriber directories

(1) Anybody gathering subscribers' personal data in order to issue a subscriber directory, whose purpose is to search for detailed contact information about persons on the basis of their names and, if applicable, other identifying elements, to the minimum extent necessary, shall:

a) inform the subscribers concerned, free of charge and before the inclusion of their data in the directory, of the purpose of the printed of electronic directory of subscribers, which is to be made available to the public either directly or through the subscriber directory inquiry services, as well as of other possibilities for its use, based on the search functions contained in the electronic versions of the directory,

b) obtain the prior consent of the subscribers to the publication of their personal data in accordance with Section 41 Subsection 5 and ensure that the subscribers have an opportunity to determine which of their personal data, from the range of information relevant for the purposes of the directory, as defined by the directory publisher, are to be included in the public directory; further, it must be ensured that the subscribers are able to verify such information and to request the amendment or removal of such information. At the same time, the person gathering such information must ensure that the subscribers can indicate, with their personal information, that they do not wish to be contacted for marketing purposes. Non-inclusion in the public directory of subscribers, the verifications, corrections and removal of information from the directory and the information concerning the subscriber's wish not to be contacted for marketing purposes shall be free of charge.

(2) If the purpose of the public directory is other than to search for detailed contact information about a person on the basis of his/her name, and, if applicable, other identifying elements, to the minimum extent necessary, anybody intending to issue such a subscriber directory must first ask for the additional consent of the subscribers concerned.

Section 96 Act on Electronic Communications

(1) It is prohibited to use electronic communications networks or services to offer any marketing advertising or any other method of offering goods or services to those subscribers who indicated in the public directory of subscribers in accordance with Section 95 Subsection 1 (b) or Section 95 Subsection 2 that they do not wish to be contacted for marketing purposes.

(2) It is prohibited to use electronic communications networks or services for the purposes of direct marketing by means of automated calling systems without human intervention (automatic calling equipment), facsimile machines or electronic mail, without the prior consent of the subscriber or user concerned.

(3) No undertaking providing subscriber directory enquiry services with information about subscriber numbers or other details may disclose any subscriber data not contained in the public directory.

(4) The provisions of Sections 95 and 96 shall apply mutatis mutandis to the data of subscribers who are legal entities.

(5) A provider of a publicly available electronic communications service, whose business interests are harmed by violations of the obligations set out in Subsections 1 to 4 above, is entitled to seek judicial protection on behalf of subscribers whose rights have been harmed by such behaviour. This does not affect the right of a party to pursue their claims in court in their own right.

The aforementioned provisions lay down in relatively detailed manner the duties of electronic communications service providers to protect substantive data (content), traffic data, and related metadata (e.g., directories) from unlawful interference. In any case, the aforementioned provisions, whenever they apply to personal data, act as *lex specialis* in relation to the Personal Data Protection Act.[69] Any subsequent forms of processing of personal data, including the rights of data subjects, limitations as to transfers of data to other jurisdictions, etc. are regulated by the Personal Data Protection Act. The subsequent applicability of the Act became apparent in a case in which a user requested traffic data from the operator of his mobile phone – his request was based on a general provision of the Personal Data Protection Act that lays down a duty on the part of a controller to inform the data subject, upon request, about any personal data thereof that are being processed. The respective provision reads as follows (informal translation):

Section 12 Personal Data Protection Act – Data subject's access to information

(1) If the data subject requests information on the processing of his personal data, the controller shall be obliged to provide him with this information without undue delay.

(2) The contents of the information shall always report on:

(a) the purpose of personal data processing;

(b) the personal data or categories of personal data that are subject of processing including all available information on their source;

(c) the character of the automated processing in relation to its use for decision-making, if acts or decisions are taken on the basis of this processing the content of which is an interference with the data subject's rights and legitimate interests;

(d) the recipients or categories of recipients.

(3) For provision of this information the controller shall be entitled to require a reasonable reimbursement not exceeding the costs necessary for provision of information.

(4) The controller's obligation to provide the data subject with information pursuant to Article 12 may be met by a processor on behalf of the controller.

Apart from providers of services of electronic communication, it should be noted that general provisions of data protection law also apply to other information society providers (e.g., online messengers, hosting providers, etc.) However, these pro-

---

[69] Act No. 101/2000 Sb., English translation available at https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1107

viders are not recognized by Czech law as telecommunication providers, so their obligations will not be dealt with here.

b) Protection of the confidentiality and integrity of information systems

The issues of confidentiality and integrity of information systems (and eventually of the third aspect of IT security, i.e., availability) do not constitute a specifically recognized constitutional principle. As noted above, they are constitutionally protected mainly through the protection of the respective systems as such (namely by the general protection of property) or by the protection of data that are stored therein (i.e., by the protection of informational self-determination, freedom of speech, freedom of scientific research, right to work, etc.).

Confidentiality and integrity, however, shape a specific part of Czech law on electronic communications. The respective provisions Act on Electronic Communications read as follows (informal translation):[70]

Section 98 Act on Electronic Communications – The security and integrity of public electronic communications networks and services

(1) An undertaking providing a public communications network or a publicly available electronic communications service shall ensure the security and integrity of its network and the security of the services it provides. For this purpose, the undertaking is, in particular, entitles to adopt technical and organisational rules created in accordance with network plans pursuant to Subsection 2. With regard to the technical capabilities of these rules to ensure a level of security that corresponds to the existing level of risk, with the aim of preventing or minimising the impact of incidents on users and of the interconnection of networks. Security of networks and services means their ability to resist random incidents or unlawful or malicious actions that seriously compromise the availability or interoperability of services and network integrity.

(2) To ensure the integrity of public communications networks, the Office shall issue network plans (Section 62), in which it defines the basic characteristics of those networks and their interfaces which are essential for the interconnection of public communications networks, for access thereto, for the connection of non-public communications networks and to ensure the continuity of provision of those services which are provided through public communications services.

(3) An undertaking providing a public electronic communications network or a publicly available electronic communications service may adopt a measure to suspend provision of the service or to deny access to the service in cases where there is a threat or occurrence of a serious breach of the security and integrity or its network as a result of damage or destruction of electronic communications facilities, mainly due to major industrial accidents or natural disasters. Such suspension or denial of service must be restricted to the time strictly necessary and, if it is technically possible, access to emergency numbers must be maintained.

(4) An undertaking providing a public electronic communications network or a publicly available electronic communications service shall immediately inform the Office, the entities operating facilities for reception of emergency calls – and, using suitable means,

---

[70] Act No. 127/2005 Sb., English translation available online at http://www.mpo.cz/dokument156553.html

also the users – about the serious breach to security and the loss of network integrity, the extent and reasons for the suspension of the services provided or the denial of access thereto, the measures adopted and of the expected time of removal of the causes pursuant to Subsection 3. The scope and form of the information to be provided shall be stipulated by the Office in an implementing legal regulation. In the event that this information is published in the public interest, the Office may inform the general public thereof in a suitable manner.

(5) Each year the Office shall submit to the Commission and the European Network and Information Security Agency (ENISA) a summary report for the previous calendar year, informing of the notifications and actions taken pursuant to Subsections 3 and 4, in the scope and format specified by the Commission.

(6) The Office may impose an obligation to carry out a safety audit on an undertaking providing a public communications network or a publicly available electronic communications service. This audit must be conducted by a qualified independent entity and the costs shall be borne by the undertaking. An undertaking providing a public communications network or a publicly available electronic communications service is also required, at the request of the Office, to submit to it the information needed to assess network security and integrity and service security, the safety audit and the results thereof.

Section 99 Act on Electronic Communications – Security, integrity and service provision in crisis situations

(1) In a crisis situation, an undertaking providing a public communications network or a publicly available electronic communications service is required, following its own technical and organisational rules, to ensure the security and integrity of its network and the interoperability of the services provided. The particulars to be included in the technical and organisational rules are stipulated by the Office in an implementing legal regulation.

(2) An undertaking referred to in Subsection 1 above shall submit to the Office at its request documents specifying the technical and organisational rules referred to in Subsection 1 above and shall allow the Office to monitor compliance with these rules. In the event any discrepancy is found between these documents and the legal regulations, the Office is entitled to inform the undertaking concerned of this fact and to set it a reasonable period within which such discrepancies are to be removed.

(3) An undertaking providing a public communications network or a publicly available telephone service is entitled, when a crisis situation is threatened or during a crisis situation39), at the request of the Ministry of Interior, to provide priority connections to the public communications network and access to the publicly available telephone service to crisis communications subscribers, in accordance with a special legal regulation. For that purpose, it is entitled, to the extent to which it is absolutely necessary, to restrict or suspend the provision of a publicly available telephone service. It shall immediately inform the Office of any restriction or suspension of a publicly available telephone service, including the scope thereof. This restriction may only be imposed for the period for which it is absolutely necessary, and access to emergency numbers must be maintained.

(4) In a crisis situation, an undertaking referred to in Subsection 1 above shall immediately inform the Office of any threat to or breaches of the security and integrity of its network and the security of services, including measures adopted or envisaged to remedy this situation and the date by which the causes are expected to be removed.

The above-cited provisions of the Act on Electronic Communications cover providers of services of electronic communication. Apart from that, the confidentiality and integrity of information systems and information networks is also subject to the

Cybersecurity Act[71] that defines its main aim, i.e., the security of information, in § 2 c) as follows (informal translation): "Security of information means ensuring confidentiality, integrity and availability of information."

Under normal circumstances, the Cybersecurity Act applies to administrators of information and communication systems belonging to a specifically listed critical information infrastructure, to administrators of important information systems (specifically listed public information systems), and to administrators of important networks (i.e., networks with direct cross-border connectivity). Regardless of their nature (i.e., private or public entities), these entities are namely obliged to implement standard security measures and to report in real-time the occurrence of cybersecurity incidents to national or governmental CERT. They also have to obey administrative orders issued by the National Security Authority *(Narodni bezpecnostni urad)*. Similar to the case of the Act on Electronic Communications, lack of compliance is considered an administrative offense.

c) Protection of the core area of privacy

The only part of Czech law where privacy *stricto sensu* is explicitly tackled is private law. However, the Civil Code, despite being adopted only in 2012, reflects neither the recently problematic nature of the concept of privacy nor its current technological determination. As a result, the Civil Code includes only very general provisions whose meanings for everyday life in today's information society is highly uncertain.

Moreover, the Civil Code introduces an extremely broad concept of an asset *(vec)* – assets are considered anything (including rights) "distinguished from an individual and useful to humans." This traditional Austro-German concept was implemented into Czech law entirely recently and thus there is a substantial lack of case law that would clarify even basic interpretative questions. In particular, it is questionable whether personal data or other data that originate in the private information sphere of an individual might be considered as "assets." On the one hand, they can be distinguished from individuals (they can exist independently), on the other, they are still strictly related to individuals. This is similar to the situation with profiles on user-generated-content services processing personal data (e.g., social networks).

The relative uncertainty of the meaning of privacy *stricto sensu* in private law leads to problematic situations in practice because even very basic disputes have to be handled as serious cases. In such cases, even standard courts have to apply the doctrine of proportionality described in II.A.2. above. For example, the Regional Court of Brno had to decide a case in which the owner of an apartment building

---

[71] Act No. 181/2014 Sb., English translation available at https://www.govcert.cz/download/nodeid-1143/

installed cameras into the entrance hall and justified their presence with the purpose of preventing theft from mailboxes. The court applied the full proportionality test and held that such an installation is not proportionate, as there are less privacy-intrusive alternatives available to achieve the same purpose (i.e., to preventively protect mailboxes).

The relatively vague nature of the meaning of the term "privacy" in Czech law (let it be constitutional or private law) causes the concept of privacy not to be used in administrative or criminal law. In particular, liability for administrative offenses and crimes is constructed upon more formally defined terms like "personal data," "traffic data," "correspondence," etc.

4. Statutory protection of personal data

a) Criminal liability for the unlawful infringement of telecommunication

The Penal Code offers a number of options that cover different possibilities of unlawful interference with communication networks. The Czech Republic is a party to the Budapest Treaty, so these provisions reflect standard types of crimes laid down therein. In particular, unlawful interference can be typically subsumed under the following crimes (full texts of respective provisions are cited *supra* II.A.2.c.):

– § 182 Violating Confidentiality of Messages
– § 230 Unauthorised Access to Computer Systems and Information Media.

It is worth noting that specific provisions of the Act on Electronic Communications and the Cybersecurity Act lay down technical requirements for providers of various telecommunication services. As a result, there is a reason to expect that such services are properly technically secured and that any unlawful interference would require overcoming certain security measures. Thus, it is also possible to sanction the unlawful interference through the possession crime aimed at devices and tools (including passwords), the aim of which is to access protected systems or networks – in particular, the Penal Code provides for § 231 Measures and Possession of Access Devices and Computer System Passwords and other such Data (full text is cited *supra* II.A.2.c.).

It can be noted, too, that Czech criminal law also sanctions preparatory activities as well as attempted crimes. The respective provisions read as follows (informal translations[72]):

Section 20 Penal Code – Premeditation

(1) Conduct that is based in an intentional creation of conditions for the commission of a particularly serious crime (Section 14 Subsection 3), especially in its organisation, the acquisition or adaptation of the means or instruments for its commission, in conspiracy,

---

[72] Act No. 40/2009 Sb., Penal Code, citation of the English translation taken from the legal information system ASPI.

unlawful assembly, in the instigation or aiding of such a crime, shall be deemed a premeditation only if the criminal law applicable for a specific criminal offence expressly stipulates for it and an attempt or completion of a particularly serious crime did not occur.

(2) Premeditation is punishable pursuant to the criminal penalty set out for a particularly serious crime to which it leads, unless the criminal law stipulates otherwise.

(3) Criminal liability for the premeditation to commit a particularly serious crime shall expire if an offender voluntarily waived further conduct towards the commission of a particularly serious crime and

a) removed the risk to an interest protected by criminal law which occurred due to the attempted premeditation, or
b) reported the premeditation to commit a particularly serious crime at a time when the risk to an interest protected by criminal law which occurred due to the attempted premeditation could still be removed; reporting must be performed to the public prosecutor or the police authority. A soldier may report it to their commander.

(4) If there are several persons involved in an act, the criminal liability for the premeditation is not void in the case of an offender who acted in such manner, despite their timely reporting or earlier participation in such act, if it is completed by other offenders.

(5) The provisions of Subsection 3 and 4 shall have no effect on the criminal liability of an offender for any other committed criminal offence which they have already committed by their conduct pursuant to Subsection 1.

Section 21 Penal Code – Attempt

(1) Any conduct that leads directly to the completion of a criminal offence and which the offender committed with the intention of the commission of a criminal offence, if the completion of the criminal offence did not occur is defined as an attempt to commit a criminal offence.

(2) An attempted criminal offence shall be punishable under the criminal penalty set for a completed criminal offence.

(3) Criminal liability for an attempted criminal offence shall expire if an offender voluntarily waived further conduct leading to the completion of a criminal offence and

a) removed the risk to an interest protected by criminal law which occurred due to the attempted criminal offence, or
b) reported the attempted criminal offence at a time when the risk to an interest protected by criminal law which occurred due to an attempted criminal offence could still be removed; reporting must be performed to the public prosecutor or the police authority. A soldier may report it to their commander.

(4) If there are several persons involved in an act, the criminal liability for an attempt is not void in the case of an offender who acted in such manner, despite their timely reporting or earlier participation in such act, if it is completed by other offenders.

(5) The provisions of Subsection 3 and 4 shall have no effect on the criminal liability of an offender for any other completed criminal offence which they have already committed by their conduct pursuant to Subsection 1.

Stored communications are protected by the criminal law namely through the crime defined in § 183 as Breach of confidentiality of documents and other privately kept documents (full text is cited *supra* II.A.2.c.). Subsequently, it is also possible to use § 230 Unauthorised access to computer systems and information media

and § 231 Measures and possession of access devices and computer system passwords and other such data.

In any case, it is relatively complicated to formulate doctrinal opinions about specific elements of the aforementioned protective provisions, as relevant case law is still lacking. For example, there have been no cases so far that would provide answers as to the applicability of § 230 or § 231 in relation to decryption keys or other tools making it possible to work with encrypted data.

b) Protection of professional secrets in criminal procedure

Czech law does not have a common denominator for professional secrets. However, certain types of data are specifically protected in criminal procedural law through the general protection of confidentiality and protection of classified information. Duties of secrecy are contained in different parts of Czech statutory law. The most important examples for the scope of this study include duties of the attorney-client privilege laid down in the Advocacy Act,[73] those defined in medical law (confidentiality of health records), banking law (confidentiality of bank account data), those defined in the Act on Electronic Communications, and those laid down in the Cybersecurity Act (secrecy of records on cybersecurity incidents). Some secrecy duties are very specific. For example, with regard to security files, i.e., personal files assembled by the National Security Authority in the course of evaluation of applicants for security clearance (i.e., for permission to handle classified information), there are only extremely exceptional cases in which, together with client data held by solicitors, these data might be used in criminal proceedings. For other types of data covered by secrecy duties, respective statutory provisions always contain relatively easily applicable procedures for the exclusion of secrecy duties.

The main provision covering the use of data where secrecy duties apply is contained in Section 8 Code of Criminal Procedure that reads as follows (informal translation):

Section 8 Code of Criminal Procedure

(1) Public authorities, legal entities and natural persons are required to comply with letters of request from law enforcement authorities for the performance of their actions without undue delay and unless a special regulation stipulates otherwise, to comply without payment. Furthermore, public authorities are also obliged to immediately notify the public prosecutor or the police authorities of facts indicating that a criminal offence has been committed.

(2) If the criminal proceedings require a proper investigation of the circumstances suggesting that a criminal offence has been committed or to assess the circumstances of the accused during court proceedings or for the enforcement of a decision, the public prosecutor and, after the indictment or a punishment petition, the presiding judge may request information that is subject to banking secrecy and data from the security register. Pursu-

---

[73] Act No. 85/1996 Sb., English translation available at http://www.cak.cz/assets/act-on-legal-profession_219_2009.pdf

ant to Section 180 of the Penal Code, the law enforcement authority may request individual data obtained under a special Act for statistical purposes during the criminal proceedings. The conditions under which the law enforcement authority may require the data obtained in the administration of taxes are stipulated under a special Act. Data obtained under this provision may not be used for a purpose other than the criminal proceedings for which such data was requested.

(3) For the reasons as stated in Subsection 2, the presiding judge may, and upon the proposal of the public prosecutor during a preliminary hearing, order the surveillance of the bank accounts or accounts of persons entitled to the records of investment instruments under a special Act for a maximum period of six months. If the reason for which the surveillance of an account was ordered exceeds this time, it may be extended upon the order of a judge from a court of higher instance and, during preliminary hearing, upon the proposal of the public prosecutor of the County Court judge for a further six months, and such prolongation can be performed repeatedly. Information obtained under this provision may not be used for a purpose other than the criminal proceedings for which it was obtained.

(4) The performance of obligations under Subsection 1 may be rejected with reference to the obligation to maintain the secrecy of classified information protected by a special Act or imposed by the State or the recognised duty of confidentiality; this does not apply,

a) if the person who has the obligation would otherwise risk criminal prosecution for the failure to notify or prevent a criminal offence, or
b) in executing the request of a law enforcement authority with regards to a criminal offence, where the requested person is also the reporter of the criminal offence.

The State recognised obligation of confidentiality under this Act does not consider such obligation the scope of which is not defined by law but instead arises from a legal action taken under the law.

(5) Unless a special Act stipulates the conditions under which information may be disclosed for the purpose of criminal proceedings that are deemed classified pursuant to such Act or which is subject to an obligation of secrecy, such information may be requested for criminal proceedings upon the prior consent of the judge. This does not affect the obligation of confidentiality of an attorney under the Advocacy Act.

(6) The provisions of Subsection 1 and 5 shall not affect the obligation of confidentiality imposed on the basis of a declared international treaty to which the Czech Republic is bound.

It is to be noted that recognised by criminal procedural law are only those secrecy duties that are laid down by statutory law (not those that are e.g. established between parties by a non-disclosure agreements).

The provision cited above might imply that the most sensitive type of data covered by secrecy duties are those of a client that are processed by his/her solicitor. Their higher level of statutory protection is based on the right to a fair trial, which also includes the right to professional representation before the court. Such representation involves the client being able to openly provide his/her solicitor with complete data about his/her case (including information that might not be favourable to her court standing). Consequently, such data have to be excluded from being available to the prosecutors or the police. Therefore, when data processed by solicitors are to be gathered and used in criminal proceedings, a special procedure involving the bar association and a court decision is required.

The so-called advocate confidentiality, namely its range and possibilities for abuse, is permanently under debate. On the one hand, solicitors tend to abuse this statutory limitation when dealing with corruption, money laundering, operations prohibited by antitrust laws, etc.[74] On the other hand, the Public Prosecution Service is constantly testing the boundaries of this statutory protection and hence raids on stored solicitor communications are not uncommon.

Recently, a highly debated case was decided in which the Public Prosecution Service requested permission to search a cloud storage facility that contained solicitor communications.[75] The respective law firm refused to provide the requested data with reference to the aforementioned "advocate confidentiality." The Public Prosecution Service requested a court warrant. The court held, however, that data stored in a cloud, i.e., off the premises of the solicitor, should not be regarded as client-solicitor communication – solicitors are obliged to keep such data under their physical control. The court considered their storage on a cloud service as a proof of the fact that these data are not to be regarded solicitor-client communication.

This decision triggered strong reactions from the Bar Association and its members, because it can be technically interpreted in a sense that data protected under "advocate confidentiality" are only those that are physically stored within the premises of respective solicitors. This would technically disable solicitors from using cloud services (even those based on specifically rented secure servers). However, the reasoning of the decision was not very specific as to the technical details under which seizure of solicitor data in the cloud is possible, so there is reason to expect further development in the case law on this matter.

c) Principle of "purpose limitation of personal data"

By the time of editing this report, the Czech Republic still has not incorporated the Police Directive[76] into its statutory law. That means the principle of purpose limitation of personal data is still explicitly incorporated only in the Czech Data Protection Act as well as in the GDPR. None of these two, however, applies on law enforcement.

---

[74] This was noted even in a decision of the Constitutional Court No. III ÚS 3988/13, available in Czech (no known English translations are available to date) at http://nalus.usoud.cz/Search/ResultDetail.aspx?id=83083&pos=1&cnt=1&typ=result

[75] Interim decision (usneseni) No. Nt 615/2014, available in Czech (no known English translations are available to date) at http://www.scribd.com/doc/235322741/Nt-615-2014

[76] See Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

The purpose limitation is laid down in Art. 4(1)(a) of the Police Directive. The proposed Data Processing Bill that shall, if passed by the two chambers of the Parliament, incorporate the Police Directive, transposes the purpose limitation in processing of personal data by law enforcement authorities (incl. Police, State Prosecution and alike) in Section 23 that reads as follows:

Section 23 Principles of processing of personal data

(1) When processing personal data, the processing authority shall

a) define particular purpose of processing of personal data in relation to particular task specified under § 22 Para 1.

b) adopt measures providing for accuracy of personal data in relation tot he nature and purpose of processing and

c) stores personal data in a form that allows for identification of data subjects only for time necessary to achieve the purpose of processing.

(2) It is possible to process personal data for a purpose unrelated to tasks referred to in § 22 Para 1 only upon specific entitlement of he processing authority and provided that the purpose is not incompatible with particular purpose laid down for respective processing.

The above provisions were strongly inspired by Arts. 4, 7 and 9 of the Police Directive. As it is not very likely that they get modified during parliamentary proceedings (there are currently no proposed amendments), we can predict they will become effective as worded above.

B. Powers in the Code of Criminal Procedure

1. Requirement of (reasonable) clarity for powers in the law of criminal procedure

As noted above, the Czech Republic has relatively long experience with situations in which the purpose of state authorities, including those involved in criminal proceedings, did not consist of much more than oppressing citizens with an incompliant political persuasion. Consequently, recently applicable limitations of powers of institutions involved in criminal proceedings are strict, and there is a general tendency to strictly and precisely outline these powers as such. A basic summary of the principles that govern Czech criminal procedure is provided in Section 2 Code of Criminal Procedure that reads as follows (informal translation[77]):

Section 2 Code of Criminal Procedure – Basic principles of criminal procedure

(1) No person shall be prosecuted other than for legitimate reasons and in a manner as stipulated by this Act.

(2) A person against whom a criminal procedure is carried out may not be perceived as guilty until the final convicting judgment of the court pronounces them as guilty.

---

[77] Act No. 141/1961 Sb., English citations taken from the information system ASPI.

(3) The public prosecutor is obliged to prosecute all criminal offences of which they learn, unless the law or a promulgated international treaty to which the Czech Republic is bound stipulates otherwise.

(4) Unless this Act stipulates otherwise, the law enforcement authorities act *ex officio*. Criminal cases must be dealt with expeditiously without undue delays; the most expeditious procedure shall be taken in particular for custody matters and the matters in which property was impounded if this is required with regard to the value and nature of the impounded property. Criminal cases shall be dealt with with a full investigation of rights and freedoms guaranteed by the Charter of Fundamental Rights and Freedoms and by international treaties on human rights and fundamental freedoms that the Czech Republic is bound by; when conducting acts of criminal proceedings, the rights of persons that such acts affect may be intervened only when justified by law and to the extent necessary to ensure the purpose of criminal proceedings. The law enforcement authorities shall not take the content of petitions affecting the performance of such obligations into account.

(5) Law enforcement authorities act in accordance with their rights and obligations under this Act and with the assistance of the parties so as to duly establish the facts of the case of which no reasonable doubt exists and to the extent that is necessary for their decisions. A confession of the accused shall not relieve the law enforcement authorities from the obligation to examine all the relevant circumstances of the case. During the preliminary hearings, the law enforcement authorities shall ascertain all the circumstances for and against the person against whom the proceeding is pending with the same care and in the manner provided by this Act even without petitions of the parties to an action. In proceedings before the court the public prosecutor and the accused may support their position with the proposal and submission of evidence. The public prosecutor must prove the guilt of the defendant. However, this does not relieve the court of the obligation to provide additional evidence to the extent required for their decision.

(6) Law enforcement authorities shall review the evidence according to their conviction based on careful consideration of all the circumstances of the case separately and as a whole.

(7) All law enforcement authorities shall cooperate with public interest groups and utilise their educational activities.

(8) A criminal prosecution before the courts is only possible on the basis of an indictment, a petition for punishment or a petition for approval of an agreement on the declaration of guilt and acceptance of punishment (hereinafter referred to as an "agreement on guilt and punishment") served by the public prosecutor. A bill of indictment in proceedings before the court is represented by the public prosecutor.

(9) In criminal proceedings before the court, decisions are made by the court or a single judge; the presiding judge or a single judge decides alone only if so expressly stipulated by the law. Should the decision during a preliminary hearing be made by a court in the first instance, then such decisions shall be made by a judge.

(10) Criminal cases are heard in public before the court so that citizens may observe and participate in hearing. At the main trial and public hearing, the public may be excluded only in cases expressly stipulated for in this Act or in a special Act.

(11) Proceedings before the courts are oral; the testimony of witnesses, experts and the accused are normally undertaken through an interrogation.

(12) When deciding during a main trial, as well as during public, custody and closed hearings, the court may only take into account evidence that was given during such proceedings.

(13) The person against whom criminal proceedings have been initiated must be instructed in every stage of the proceedings in an appropriate and comprehensible manner

as to their rights granting them the full use of defence and that they may choose their defence counsel; all law enforcement authorities are required to enable them to exercise their rights.

(14) Law enforcement authorities conduct the proceedings and produce decisions in the Czech language. Any person who declares that they do not speak Czech is entitled to speak their mother tongue or a language that they indicate they can speak to the law enforcement authorities.

(15) At every stage of the proceedings the law enforcement authorities are obliged to make it possible for the victim to fully exercise their rights and are also obliged to instruct the victim of the victim's rights in an appropriate and comprehensible manner under the law so that the victim can achieve satisfaction of their claims; the proceedings must be conducted with the required consideration for the victim and while being duly regardful of their person.

The need for strict clarity of powers was also one of main reasons why the Constitutional Court quashed the former implementation of data retention obligations, as it contained only general formulations instead of an explicit list of institutions entitled to ask for retained traffic data and the precise establishment of respective procedures, explicitly including the possibility of judicial review. The Court ruled (official translation[78]):

37. In its judgments, the conditions outlined above have been specified by the Constitutional Court when assessing the admissibility of the intervention of the public authority to individual privacy taking the form of telecommunication operation interception [cf. e.g. the quoted Judgments file reference II. ÚS 502/2000, file reference IV. ÚS 78/01, file reference I. ÚS 191/05, or file reference I. ÚS 3038/07 issued on 29 February 2008 (N 46/48 SbNU 549)]. The infringement of the individual's fundamental right to privacy in the form of the right to informational self-determination in the sense of Article 10, para. 3 and Article 13 of the Charter, due to the prevention of and protection against criminal activity is thus possible only by means of imperative legal regulations which have to conform to, above all, the rights arising from the principle of the legal state (rule of law state) and which meet the requirements arising from the proportionality test when, in the case of a conflict between the fundamental rights and freedoms with the public interest or any other fundamental rights and freedoms, the purpose (objective) of such infringement must be assessed in relation to the means applied, whereas it is the proportionality principle (in a broader sense) that provides the standard for such assessment. The wording of such legal regulations must be precise and unambiguous, while also being sufficiently predictable so that it provides potentially affected individuals with sufficient information on the circumstances and conditions under which the public authority is entitled to interfere with their privacy and so that they can act accordingly in order to avoid conflict with the restricting norm. Moreover, the powers granted to the relevant authorities, as well as the manner and the rules of application, must be strictly defined so that individuals are provided with protection against arbitrary infringements. From the perspective of the proportionality principle (in a broader sense), assessing the admissibility of the infringement in question includes three criteria. The first one lies in assessing the eligibility of fulfilling the purpose (or appropriateness as well), where it is determined whether the specific measure itself is capable of achieving the intended purpose, being the protection of another fundamental right or public interest. The second criterion consists in assessing the necessity, i.e. examining whether, upon selecting the

[78] Decision No. Pl. ÚS 24/10, English translation available at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=c574142df486769e0b435954fead08c3

appropriate means, the one being most considerate of the fundamental right has been opted for. And finally, it is necessary to assess the adequacy (in a narrower sense), i.e. whether the prejudice to the fundamental right is not disproportionate in relation to the intended purpose, which means that the measures imposing a restriction on fundamental rights and freedoms must not, in case of a collision of the fundamental right or freedom with public interest, exceed (through their negative consequences) the positive aspects represented by the public interest in these measures [cf. the Judgment file reference Pl. ÚS 3/02 issued on 13 August 2002 (N 105/27 SbNU 177; 405/2002 Sb.)].

[…]

51. Under no circumstances may the stipulation of the duty imposed on legal entities or natural persons to secure that "the content of message should not be retained together with the defined data" (Section 97, para. 3, sentence four) or the duty to "eliminate them upon the expiration of the period unless they have been provided to the competent authorities in compliance with a special legal regulation or unless stated otherwise within the Act (Section 90)" (Section 97, para. 3, sentence six) be deemed by the Constitutional Court as providing sufficient, unambiguous, detailed and appropriated guarantees. The retention period itself, "no shorter than 6 months and longer than 12 months", the expiration of which determines the obligation to remove the data, can also be deemed as ambiguous and totally insufficient with respect to the extent and sensitivity of the retained data. None of these obligations is provided, in more detail, with the rules and specific procedures for how to meet them; the requirements concerning the security of the retained data have not been defined in a stringent manner; it is not sufficiently clear how the data are handled, either by legal entities or natural persons collecting and retaining the location and traffic data, or by the competent public authorities when requested; and the manner in which the data are removed has not been specifically determined either. Similarly, the liability or possible sanctions for failure to comply with such duties, including the absence of the possibility for the individuals affected to seek efficient protection against potential misuse, arbitrariness or failure to comply with the relevant duties have not been defined either. Supervision provided by the Office for Personal Data Protection, as anticipated in the Act on Electronic Communications (Section 87 and further), "over observing the duties and obligations when processing personal data" or the corresponding instruments of its activities and monitoring cannot be considered as an adequate and effective means of protecting the fundamental rights of the individuals affected, since they do not control the instrument by themselves [see the Judgment file reference Pl. ÚS 15/01 issued on 31 October 2001 (N 164/24 SbNU 201; 424/2001 Sb.) where appropriate]. As a consequence, the actions referred to above, constituting an obvious infringement of the fundamental right to privacy in the form of the right to informational self-determination (in the sense of Article 10, para. 3 and Article 13 of the Charter) and due to the legal regulation being considered as insufficient and failing to meet the afore-mentioned constitutional requirements, occur beyond the scope or reach of any immediate (yet subsequent) review, particularly a judicial one, the necessity of which has also been expressed by the ECHR in the Decision concerning the case of Camenzind v. Switzerland, referred to above.

It should be noted that the Public Prosecution Service and the police had internally implemented relatively strict procedures that provided for case-by-case precise documentation of each request and that also included court orders (despite that this procedure is not prescribed by the law). Consequently, retained data that had been used in certain prior cases did not have to be declared inadmissible evidence.

Lack of clarity was also the main reason for the above-cited Constitutional Court decision repealing former provisions Code of Criminal Procedure that provided for

a competence on the part of the Public Prosecutor to request retained data. In that case, the Court ruled:[79]

> 24. The wording of the contested provision implies that the order for disclosure of the telecommunication traffic data is only expressly conditioned by the fact that such measures must pursue the goal of "clarification of the circumstances significant for criminal proceedings". The Constitutional Court believes that the limits of the fundamental right to informational self determination regulated in this manner are formulated too widely and vaguely, and in essence, they allow the relevant data to be requested and used by the bodies active in criminal proceedings each time a certain connection with the on-going criminal proceedings may be associated with them. At the same time, the Court is aware of the obligation of public authorities to apply sub-constitutional legal regulations in compliance with the constitutional order, which in this case implies their duty to examine, in every specific matter, whether apart from identifying the telecommunication traffic data of a specific person there is not, in respect to the seriousness of the criminal offence, any other possibility to achieve the goal of the criminal proceedings otherwise or whether it does not amount to an inadequate interference with the individual's fundamental right. It also considers important that the protection of fundamental rights and freedoms is subject to, in every individual case, review of an independent and impartial court, since decision making on issuing the relevant order is granted by the contested provision to the presiding judge or the judge within the preliminary proceedings, whereas such orders must be issued in writing and accompanied with reasoning. Nevertheless, these are guarantees that allow protection to be provided against an inadequate interference with the right to informational self-determination with respect to the facts of a particular case, yet they cannot eliminate the deficiencies consisting in indefiniteness and too general a character of the contested legal regulation in such a way that they would replace, on their own and in general terms, the consideration of the legislature on the intensity of a certain public interest in restricting a fundamental right or freedom in the case of individual criminal offences and the manner (i.e. specific form) of such restriction, including the afore-mentioned subsequent guarantees when disposing of the relevant data, which represent a political decision adopted within the limits defined by the constitutional order, with their own detailed abstract consideration. If adopted by courts, this approach would also be inconsistent with Art. 4, para. 2 of the Charter, pursuant to which limitations of the fundamental rights and freedoms may be placed upon them only by law, since only the legislature is provided with the constitutional capacity, upon imposing a certain duty, to give preference, at its own discretion and while respecting the proportionality principle, of the public interest approved by the constitutional order to the fundamental right in a type-defined legal relation. Furthermore, leaving the determination of the constitutionally constituent limits only on the decision-making practice of courts would not be consistent with the requirement of legal certainty, since any potential interference with the right to informational self-determination is not, as a consequence of the indefiniteness of the current legal regulation, predictable for the individual to such an extent that would correspond to the seriousness of any possible negative effects onto their privacy. It may thus be stated that it is this indefiniteness that represents the primary deficiency of the contested legal regulation, as far as its constitutional review is concerned.

---

[79] Decision No. Pl. ÚS 24/11, English translation available at http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/decisions/pdf/Pl_US_24-11.pdf

2. Differentiation and classification of powers in the law of criminal procedure

Coercive powers related to telecommunication data are relatively precisely defined in criminal procedure. In this respect, Czech law is relatively specific with its bilateral regulation of wiretapping and retention of traffic data. This means that duties and procedures which apply to providers of electronic communications services are defined in Act on Electronic Communications, while procedures that apply to the police or Prosecution Service are laid down in the Code of Criminal Procedure. The reason for this dichotomy is that wiretapping and data retention also serve other purposes than just criminal procedure. Consequently, provisions laid down in the Act on Electronic Communications cover the obligations of providers of services of electronic communications in general and specify only purposes for which respective data might be requested. Procedures for requesting these data are then laid down in specific acts (incl. the Code of Criminal Procedure).

The respective provisions of the Act on Electronic Communications read as follows (informal translation[80]):

Section 97 Act on Electronic Communications

(1) A legal entity or natural person providing a public communications network or a publicly available electronic communications service shall, at the expense of the requesting party, provide and secure interfaces at specified points of the network to connect terminal equipment for message tapping and recording:

a) for the Police of the Czech Republic for the purposes specified in a special legal regulation,

b) for the Security Information Service for the purposes specified in a special legal regulation,

c) for the Military Intelligence service for the purposes specified in a special legal regulation.

(2) The bodies listed in Subsection 1 above shall prove their authorisation for message tapping and recording by submitting a written application, which contains a reference number under which the court ruling is filed by this body, and which is signed by the person responsible from the body listed in Subsection 1 above for the performance of the message tapping and recording. In the event of message tapping and recording by the Police of the Czech Republic in accordance with special legal regulations) the written application shall contain a reference number under which the consent of the user of the station monitored is filed by the Police of the Czech Republic.

(3) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service shall for a period of 6 months traffic and location data which are created or processed during the operation of their public communications networks and during the provision of their publicly available electronic communications services. A legal entity or a natural person providing a public communications network or a publicly available electronic communications service is only required to store data relating to unsuccessful call attempts only when these data are creat-

[80] Act No. 127/2005 Sb., English translation available online at http://www.mpo.cz/dokument156553.html

ed or processed and at the same time stored or recorded. At the same time, such a legal entity or natural person is required to ensure that, during the performance of the obligation referred to in the first and second sentences, no message content has been stored, and that no content thus stored has been further distributed. A legal entity or a natural person who stores traffic and location data is required, on request, immediately to provide them to:

a) criminal law enforcement authorities for the purposes of and under the conditions laid down in a special legal regulation,
b) the Police of the Czech Republic for the purposes of initiating a search for a specific wanted or missing person, for the identification of persons of unknown identity or the identity of a corpse that has been discovered, for the prevention or detection of specific terrorist threats or for the verification of a protected person, while complying with the conditions set out in a special legal regulation,
c) the Security Information Service, for the purposes of and under the conditions laid down in a special legal regulation,
d) the Military Intelligence service for the purposes of and under the conditions laid down in a special legal regulation,
e) the Czech National Bank for the purposes of and under the conditions laid down in a special legal regulation.

After expiry of the period referred to in the first sentence above, the legal entity or natural person who stores the traffic and location data is required to destroy them, unless they were provided to the bodies authorised to use them under a special legal regulation, or unless otherwise provided in this Act (Section 90).

(4) The traffic and location data pursuant to Subsection 3 above are primarily data leading to the tracing and identification of the source and address of the communication, and also data leading to the identification of the date, time, method and duration of the communication. The scope of the traffic and location data stored in accordance with Subsection 3 above, the form and method of their transmission to the bodies authorised to use them under a special legal regulation, and the method of their disposal is stipulated in an implementing legal regulation.

(5) A legal entity or natural person providing a publicly available telephone service is required, on request, to provide information from the database of all its subscribers to the publicly available telephone service to a body authorised to request them in accordance with a special legal regulation, at their own expense. The form and scope of the information provided is stipulated in an implementing legal regulation.

(6) Where a legal entity or natural person providing a public communications network or a publicly available electronic communications service introduces into its activities any coding, compression, encryption or any other method of transmission that makes the messages being transmitted incomprehensible, such a person shall ensure that the messages requested and the traffic and location data related thereto are provided in a comprehensible manner at the termination points for connection of the terminal equipment referred to in Subsection 1 above.

(7) For fulfilling the obligations specified in Subsections 1, 3 and 5 above, the legal entity or natural person is entitled to reimbursement for effectively incurred costs from the authorised body which requested or ordered such an action. The amount and method of reimbursement for the effectively incurred costs is set out in an implementing legal regulation.

(8) A person referred to in Subsection 1 above and its employees are required to maintain the confidentiality of any tapping or recording of messages requested or implemented in accordance with Subsections 1 and 2 and data requested or provided in accordance with Subsections 3 and 5 and matters related thereto.

(9) The technical and operational conditions and points for the connection of terminal telecommunications equipment for the tapping or recording of messages is set out in an implementing legal regulation.

(10) A legal entity or natural person providing a public communications network or a publicly available electronic communications service shall keep records on:

a) the number of cases where, on requested, it provided traffic and location data to the bodies authorised to request them,

b) the period that elapsed, in each case, from the date on which the storage of the traffic and location data began to the date on which the authorised body requested such data, and

c) the number of cases when it was not able to comply with a request to provide traffic and location data.

(11) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service is required to provide to the Office the collective records referred to in Subsection 10 above, for the previous calendar, in electronic form, at the latest by 31 January of the following calendar year. The records provided may not contain personal and identification data. The Office shall immediately send the collective records received to the Commission.

(12) The form of the records provided under Subsection 11 and the method of their submission to the Office is stipulated in an implementing legal regulation.

The respective provisions Code of Criminal Procedure read as follows (informal translation[81]):

Section 88 Code of Criminal Procedure

(1) If criminal proceedings are conducted for a crime for which the law stipulates a prison sentence with the upper penalty limit of at least eight years, for a criminal offence of machinations in insolvency proceedings under Section 226 of the Penal Code, violation of regulations on rules of competition under Section 248 Subsection 1 Paragraph e) and Subsection 2 through 4 of the Penal Code, negotiating advantages during public procurement, tender and auction under Section 256 of the Penal Code, machinations during public procurement and tenders under Section 257 of the Penal Code, machinations at a public auction under Section 258 of the Penal Code, misuse of powers of an official person under Section 329 of the Penal Code or for any other intentional criminal offence for which prosecution is stipulated in a declared international treaty, an order for the interception and recording of telecommunications may be issued if it may be reasonably assumed that facts relevant to the criminal proceedings will be obtained in this way and if there is no other way to achieve such purpose or if its achievement would be otherwise significantly reduced. The Police of the Czech Republic perform the interception and recording of telecommunications for the needs of all law enforcement authorities. The interception and recording of telecommunications between the defence counsel and the accused is inadmissible. If the police authority finds during the interception and recording of telecommunications that the accused has communicated with their defence counsel, they are obliged to immediately destroy the interception recording and not to use the information learned in this context in any way. The report on the destruction of the record shall be placed in the file.

(2) The presiding judge and, in preliminary proceedings upon the petition of the public prosecutor, the judge, is entitled to warrant the interception and recording of telecommunications. If there is a criminal proceeding for an intentional criminal offence, the

---

[81] Act No. 141/1961 Sb., English citations taken from the information system ASPI.

prosecution of which is governed by the applicable international treaty, the order for the interception and recording of telecommunications must be issued in writing and must be justified, including a specific reference to the applicable international treaty. The order for the interception and recording of the telecommunications service shall include a determined user address or a user device and the user if their identity is known, and the period during which the interception and recording of telecommunications traffic is conducted cannot be longer than four months; the justification must include the specific facts that justify the issue of such order as well as its period. The order for the interception and recording of telecommunications shall immediately be forwarded to the police authority. In the preliminary hearing, the judge shall send a copy of the order for the interception and recording of telecommunications to the public prosecutor without undue delay.

(3) The police authority is obliged to continuously assess whether the reasons which led to an order for the interception and recording of telecommunications are still valid. If the reasons have expired, they are obligated to immediately terminate the interception and recording of telecommunications even before the end of the period referred to in Subsection 2. They will immediately notify the presiding judge in writing, who issued the order for the interception and recording of telecommunications, and in the preliminary hearing, the public prosecutor and the judge.

(4) Based on the assessment of the current course of the interception and, recording of telecommunications, the judge of a superior court and, in the preliminary hearing upon the petition of the public prosecutor, deputy county court judge may extend the duration of the interception and recording of telecommunications traffic even repeatedly, however, always only for a maximum period of four months.

(5) The law enforcement authority may, without the order for the interception and recording of telecommunications, order the interception and recording of telecommunications or conduct it themselves if there is a criminal proceeding for the criminal offence of human trafficking (Section 168 of the Penal Code), the delegation of custody of a child to someone else (Section 169 of the Penal Code), restriction of personal freedoms (Section 171 of the Penal Code), extortion (Section 175 of the Penal Code), kidnapping of a child and persons suffering from a mental disorder (Section 200 of the Penal Code), violence against a group of people or an individual (Section 352 of the Penal Code), dangerous threats (Section 353 of the Penal Code) or dangerous persecution (Section 354 of the Penal Code), if the user of the intercepted unit agrees to such measure.

(6) If the record of the telecommunications service is to be used as evidence, it is necessary to accompany it with the transcript, giving the place, time, manner and contents of the record, as well as the authority which issued the record. The police authority is obliged to label other records, securely store them so as to protect them against unauthorised misuse, and indicate the place of storage in the transcript. In another criminal case other than the one in which the interception and recording of telecommunications service was performed, the recording may be used as evidence if there is a criminal prosecution in this matter for a criminal offence referred to in Subsection 1, or with the consent of the user by the intercepted station.

(7) If the interception and recording of the telecommunications service did not find any facts relevant to the criminal proceedings, the police authority, after approval by a court and in preliminary hearings, the public prosecutor, must immediately destroy all records after three years from the final conclusion of the matter. If the police authority was informed of an extraordinary appeal within the set deadline, they shall destroy the records of the interception after the decision on the extraordinary appeal or after a final conclusion on the matter. The police authority shall send a transcript on the destruction of the record of the interception to the public prosecutor, whose decision finally concluded the

matter and in proceedings before the court, to the presiding judge in the first instance, for the record on file.

(8) The public prosecutor or the police authority, by whose decision the case was finally concluded, and in proceedings before the court the presiding judge in the first instance after the final conclusion of the matter, shall inform the person referred to in Subsection 2, if known, on the ordered interception and recording of telecommunications service. The information includes the designation of the court that issued an order for the interception and recording of telecommunications service, the duration of the interception and the date of the conclusion. Part of the information includes the instructions on the right to submit, within six months of receipt of this information, a petition to review the legality of the order for the interception and recording of telecommunications service to the Supreme Court. The presiding judge of the court in the first instance shall submit the information without undue delay after the final conclusion of the matter, the public prosecutor by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the Attorney General under Section 174a and the police authority by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the public prosecutor under Section 174 Subsection 2 Paragraph e).

(9) The presiding judge, the public prosecutor or the police authority does not submit the information under Subsection 8 in proceedings on a crime committed by an organised group for which the law stipulates a prison sentence with the upper penalty limit of at least eight years, in proceedings on criminal offences committed for the benefit of an organised criminal group, in proceedings for criminal participation in an organised criminal group (Section 361 of the Penal Code), or if the criminal offence involved more people and in relation to at least one of them the criminal proceedings have not yet been finally concluded or if it is against the person to whom the information was submitted, is the subject of criminal proceedings, or if providing such information could defeat the purpose of the criminal proceedings, including those referred to in Subsection 6, or if it could lead to threats to national security, life, health, or the rights and freedoms of individuals.

Section 88a Code of Criminal Procedure

(1) If, for the purposes of criminal proceedings conducted for an intentional criminal offence for which the law sets out a prison sentence with an upper penalty limit of at least three years, for the criminal offence of violating the confidentiality of messages (Section 182 of the Penal Code), for the criminal offence of fraud (Section 209 of the Penal Code), for the criminal offence of unauthorised access to computer systems and information media (Section 230 of the Penal Code), for the criminal offence of procuring and possessing access devices and computer system passwords and other such data (Section 231 of the Penal Code), for the criminal offence of dangerous threats (Section 353 of the Penal Code), for the criminal offence of dangerous persecution (Section 354 of the Penal Code), for the criminal offence of spreading alarming news (Section 357 of the Penal Code), for the criminal offence of encouraging a criminal offence (Section 364 of the Penal Code), for the criminal offence of approving a criminal offence (Section 365 of the Penal Code) or for an intentional criminal offence for which prosecution is stipulated in a proclaimed international treaty binding on the Czech Republic, it is necessary to ascertain data on the telecommunications service that are the subject of a telecommunications secret or that are subject to the protection of personal and intermediation data, and there is no other way to achieve the pursued purpose or if its achievement would be otherwise significantly harder, their release to the public prosecutor or to the police authority shall be ordered by the presiding judge in proceedings before the court and by the judge upon the petition of the public prosecutor in a preliminary hear-

ing. If there are criminal proceedings for a criminal offence the prosecution of which is stipulated in such international treaty, the order for ascertaining data on the telecommunications service must be issued in writing and must be justified, including a specific reference to the proclaimed international treaty. If the request applies to a particular user, their identity must be stated in the order, if known.

(2) The public prosecutor or the police authority by whose decision the matter was finally concluded, and in proceedings before the court the presiding judge of the court of first instance after the final conclusion of the matter, shall inform the user referred to in Subsection 1, if known, of the ordered ascertainment of data on the telecommunications service. The information shall identify the court which issued the order for the ascertainment of data on the telecommunications service, and detail the period to which such order applied. Such information shall include instructions on the right to submit to the Supreme Court, within six months of receipt of this information, a petition to review the legality of the order for the ascertainment of data on the telecommunications service. The presiding judge of the court of first instance shall submit the information without undue delay after the final conclusion of the matter, the public prosecutor by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the Attorney General under Section 174a, and the police authority by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the public prosecutor under Section 174 Subsection 2 Paragraph e).

(3) The presiding judge, the public prosecutor or the police authority shall not submit the information under Subsection 2 in proceedings on a crime committed by an organised group for which the law stipulates a prison sentence with an upper penalty limit of at least eight years, in proceedings on a criminal offence committed for the benefit of an organised criminal group, in proceedings on the criminal offence of participation in an organised criminal group (Section 361 of the Penal Code), or if the commission of the criminal offence involved several persons and in relation to at least one of them criminal proceedings have not yet been finally concluded or if criminal proceedings are conducted against the person to whom the information is to be submitted, or if providing such information could defeat the purpose of the particular or some other criminal proceedings, or if it could threaten national security, life, health, or the rights or freedoms of individuals.

(4) An order under Subsection 1 is not required if the user of the telecommunications equipment to whom the data on the performed telecommunications service relates gives their approval for the provision of the information.

It is to be noted that, despite formally having the opportunity to request wiretapping or retained traffic data, the police has *de facto* extremely limited options to use this coercive power in criminal proceedings. As a result, no situations occur in practice in which the police would directly request wiretapping or traffic data for the purpose of criminal procedure – if the respective data are needed in criminal procedings, such requests are always made through the Public Prosecution Office.

As noted above in II.A.3., there are, apart from traffic data, no distinct procedural rules for specific coercive powers to obtain stored communications. Consequently, stored communications are gathered and forensically exploited based upon general rules enabling the police or the Public Prosecution to secure assets, request information, conduct surveillance, etc. The use of these powers is discussed in detail in III. below.

III. Powers for Accessing Telecommunication Data in the Law of Criminal Procedure

A. Overview

The most important regulation for interception of electronic communications and for otherwise accessing electronic communications data for the purpose of criminal investigations is contained in the Code of Criminal Procedure.[82]

There are two specific provisions Code of Criminal Procedure, which allow law enforcement authorities to intercept electronic communications and to access electronic communications data for the purpose of criminal investigations – Sections 88 and 88a.

The first of these lays down rules for the interception and recording of telecommunication and the second one for the accessing of data on telecommunication services, which are subject to telecommunication secrecy or subject to the protection of personal and intermediation data. Section 88 basically allows law enforcement authorities to intercept and record the content of data transmission in real time under specified conditions in criminal proceedings, whereas Section 88a allows them to access traffic and location data under specified conditions, which must be retained by entities providing a public communications network[83] or publicly available electronic communications service[84] (ISPs) in accordance with the Act on Electronic Communications.[85]

Since there are no other specific rules for specific coercive powers to obtain stored data, communication stored by the user or the ISP is being accessed and processed under more general provisions, which allow law enforcement authorities to obtain (either voluntarily or upon request, according to Section 78 Code of Criminal Procedure) or seize (Section 79 Code of Criminal Procedure) devices and storage mediums in which the data are stored; to conduct surveillance (Section 158d Code of Criminal Procedure) of persons and assets, upon which the data may be gathered; or to request respective information or data using a production order (Section 8 Code of Criminal Procedure).

---

[82] Act No. 141/1961 Sb. Code of Criminal Procedure.

[83] Electronic communications network used wholly or mainly for the provision of publicly available electronic communications services, which support the transfer of information between end nodes of the network. See Section 2 Act on Electronic Communications.

[84] Publicly available service normally provided for remuneration, which consists wholly or mainly in the transfer of signals via electronic communications networks. See Section 2 of the Act on Electronic Communications.

[85] Act No. 127/2005 Sb. on electronic communications and amending certain related laws (the Act on Electronic Communications).

The same instruments are also used in practice to discover and gather not only media, but also mere (intangible) data. The use of these general instruments that were originally legislated for tangible assets, is already relatively settled but it still remains quite problematic. Moreover, there is up to date no statutory instrument for quick-freeze for law enforcement.

Both the fact that data are being gathered upon instruments originally legislated for tangible assets and that there is still missing procedural instrument for quick-freeze, raise questions over compliance of the Czech criminal procedure with the Budapest treaty. In addition, if EU Production and Preservation Orders are introduced, it might be very problematic for Czech courts and police authorities to estsablish procedural causes namely for Preservation Orders.

Thus, an amendment to the Code of Criminal Procedure was recently (Fall 2018) put to the legislative pipeline. The amendment aims at introducing more particular procedural instruments for seizure of stored data and allowing for quick-freeze orders (preservation orders).

Czech law contains also other statutes that deal with interception or are somehow important for it, primarily Act No. 127/2005 Sb. on electronic communications and its implementing regulations, Act No. 273/2008 Sb. on the Police of the Czech Republic, and Act No. 85/1996 Sb. on advocacy. These acts will be described in more detail below.

B. Interception of Content Data

1. Statutory provision

As in most countries, the Czech Republic has one main provision in the law of criminal procedure, which deals with the interception of the content of communication in transmission – Section 88 Code of Criminal Procedure.[86] Below is the wording of the entire provision (informal English translation[87]):

Section 88 Code of Criminal Procedure – Interception and recording of telecommunications

(1) If criminal proceedings are conducted for a crime for which the law stipulates a prison sentence with the upper penalty limit of at least eight years, for a criminal offence of machinations in insolvency proceedings under Section 226 of the Penal Code, violation of regulations on rules of competition under Section 248 Subsection 1 Paragraph e) and Subsection 2 through 4 of the Penal Code, negotiating advantages during public procurement, tender and auction under Section 256 of the Penal Code, machinations during public procurement and tenders under Section 257 of the Penal Code, machinations at a

---

[86] For a detailed analysis of respektive legislative provisions and related case-law, see Polčák, R., Púry, F., Harašta, J. Elektronické důkazy v trestním řízení. Brno : Masarykova univerzia, 2015.

[87] Act No. 141/1961 Sb., English citations were taken from the information system ASPI.

public auction under Section 258 of the Penal Code, misuse of powers of an official person under Section 329 of the Penal Code or for any other intentional criminal offence for which prosecution is stipulated in a declared international treaty, an order for the interception and recording of telecommunications may be issued if it may be reasonably assumed that facts relevant to the criminal proceedings will be obtained in this way and if there is no other way to achieve such purpose or if its achievement would be otherwise significantly reduced. The Police of the Czech Republic perform the interception and recording of telecommunications for the needs of all law enforcement authorities. The interception and recording of telecommunications between the defence counsel and the accused is inadmissible. If the police authority finds during the interception and recording of telecommunications that the accused has communicated with their defence counsel, they are obliged to immediately destroy the interception recording and not to use the information learned in this context in any way. The report on the destruction of the record shall be placed in the file.

(2) The presiding judge and, in preliminary proceedings upon the petition of the public prosecutor, the judge, is entitled to warrant the interception and recording of telecommunications. If there is a criminal proceeding for an intentional criminal offence, the prosecution of which is governed by the applicable international treaty, the order for the interception and recording of telecommunications must be issued in writing and must be justified, including a specific reference to the applicable international treaty. The order for the interception and recording of the telecommunications service shall include a determined user address or a user device and the user if their identity is known, and the period during which the interception and recording of telecommunications traffic is conducted cannot be longer than four months; the justification must include the specific facts that justify the issue of such order as well as its period. The order for the interception and recording of telecommunications shall immediately be forwarded to the police authority. In the preliminary hearing, the judge shall send a copy of the order for the interception and recording of telecommunications to the public prosecutor without undue delay.

(3) The police authority is obliged to continuously assess whether the reasons, which led to an order for the interception and recording of telecommunications are still valid. If the reasons have expired, they are obligated to immediately terminate the interception and recording of telecommunications even before the end of the period referred to in Subsection 2. They will immediately notify the presiding judge in writing, who issued the order for the interception and recording of telecommunications, and in the preliminary hearing, the public prosecutor and the judge.

(4) Based on the assessment of the current course of the interception and, recording of telecommunications, the judge of a superior court and, in the preliminary hearing upon the petition of the public prosecutor, deputy county court judge may extend the duration of the interception and recording of telecommunications traffic even repeatedly, however, always only for a maximum period of four months.

(5) The law enforcement authority may, without the order for the interception and recording of telecommunications, order the interception and recording of telecommunications or conduct it themselves if there is a criminal proceeding for the criminal offence of human trafficking (Section 168 of the Penal Code), the delegation of custody of a child to someone else (Section 169 of the Penal Code), restriction of personal freedoms (Section 171 of the Penal Code), extortion (Section 175 of the Penal Code), kidnapping of a child and persons suffering from a mental disorder (Section 200 of the Penal Code), violence against a group of people or an individual (Section 352 of the Penal Code), dangerous threats (Section 353 of the Penal Code) or dangerous persecution (Section 354 of the Penal Code), if the user of the intercepted unit agrees to such measure.

(6) If the record of the telecommunications service is to be used as evidence, it is necessary to accompany it with the transcript, giving the place, time, manner and contents of the record, as well as the authority, which issued the record. The police authority is obliged to label other records, securely store them so as to protect them against unauthorised misuse, and indicate the place of storage in the transcript. In another criminal case other than the one in which the interception and recording of telecommunications service was performed, the recording may be used as evidence if there is a criminal prosecution in this matter for a criminal offence referred to in Subsection 1, or with the consent of the user by the intercepted station.

(7) If the interception and recording of the telecommunications service did not find any facts relevant to the criminal proceedings, the police authority, after approval by a court and in preliminary hearings, the public prosecutor, must immediately destroy all records after three years from the final conclusion of the matter. If the police authority was informed of an extraordinary appeal within the set deadline, they shall destroy the records of the interception after the decision on the extraordinary appeal or after a final conclusion on the matter. The police authority shall send a transcript on the destruction of the record of the interception to the public prosecutor, whose decision finally concluded the matter and in proceedings before the court, to the presiding judge in the first instance, for the record on file.

(8) The public prosecutor or the police authority, by whose decision the case was finally concluded, and in proceedings before the court the presiding judge in the first instance after the final conclusion of the matter, shall inform the person referred to in Subsection 2, if known, on the ordered interception and recording of telecommunications service. The information includes the designation of the court that issued an order for the interception and recording of telecommunications service, the duration of the interception and the date of the conclusion. Part of the information includes the instructions on the right to submit, within six months of receipt of this information, a petition to review the legality of the order for the interception and recording of telecommunications service to the Supreme Court. The presiding judge of the court in the first instance shall submit the information without undue delay after the final conclusion of the matter, the public prosecutor by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the Attorney General under Section 174a and the police authority by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the public prosecutor under Section 174 Subsection 2 Paragraph e).

(9) The presiding judge, the public prosecutor or the police authority does not submit the information under Subsection 8 in proceedings on a crime committed by an organised group for which the law stipulates a prison sentence with the upper penalty limit of at least eight years, in proceedings on criminal offences committed for the benefit of an organised criminal group, in proceedings for criminal participation in an organised criminal group (Section 361 of the Penal Code), or if the criminal offence involved more people and in relation to at least one of them the criminal proceedings have not yet been finally concluded or if it is against the person to whom the information was submitted, is the subject of criminal proceedings, or if providing such information could defeat the purpose of the criminal proceedings, including those referred to in Subsection 6, or if it could lead to threats to national security, life, health, or the rights and freedoms of individuals.

2. Scope of application

a) Object of interception

The object of interception is broadly specified as "telecommunication traffic." Neither the legislature nor case law deals with a definition of this term. Traditionally, this term means communication between persons via landlines, mobile phones, fax, radio, or similar devices. However, due technological developments, the interpretation of this term is changing. Nowadays, it would probably cover all sorts of communication transferred via telecommunication and electronic communications networks, including communication between computers or other communication devices as well as any kind of IP traffic, regardless of whether it was generated by persons or computers. Even content data transferred while surfing the web using electronic communications networks may be the object of interception.

When defining the term "telecommunication traffic," the literature usually refers to the Act on Electronic Communications.[88] The act itself does not contain a definition of the term, but we may understand it as meaning content transferred via electronic communications networks, which are defined by the act as transmission systems and, where applicable, switching or routing equipment and other facilities, including network elements that are inactive and that permit the transmission of signals.[89]

Another implication may be found elsewhere in the Act on Electronic Communications, specifically in Section 89, which deals with the confidentiality of communication (informal translation[90]):

Section 89 Act on Electronic Communications – Confidentiality of communication

(1) Undertakings providing a public communications network or a publicly available electronic communications service shall implement technical and organisational measures to safeguard the confidentiality of the messages and the related traffic and location data, which are transmitted via their public communications network and the publicly available electronic communications services. In particular, such undertakings shall not admit any tapping, message storage, or any other types of interception or monitoring of messages, including the data contained therein and related thereto, by any persons other than the users, without the consent of the users concerned, unless otherwise provided in an Act. This shall not be to the prejudice of the technical storage of data as needed for message transmission without affecting the confidentiality principle.

(2) A message means any information being exchanged or transmitted between a finite number of subscribers or users via the publicly available electronic communications service, except for the information transmitted as part of the public radio or television broadcasting service via the electronic communications network, unless it can be allocated to an identifiable subscriber or user receiving that information.

---

[88] For example, Šámal, Pavel. Trestní řád: komentář. 7., extended release. In Prague: C.H. Beck, 2013, Velké komentáře.

[89] Section 2 letter h) of Act No. 127/2005 Sb. on electronic communications.

[90] Act No. 127/2005 Sb., English translation available online at http://www.mpo.cz/dokument156553.html

Thus, according to the provision cited above and other references, we may conclude that telecommunication traffic may be defined as any data transferred via public electronic communications networks between a finite number of subscribers or users. Since it is impossible to tell in advance whether intercepted electronic communications will or will not contain such data, any interception should take place only after the interception order has been issued.

b) Temporal limits of telecommunication

aa) Access to ongoing telecommunication

Access to ongoing electronic communications is definitely covered by the abovementioned provision. The police may, upon receiving the interception order, intercept any data that are "in traffic" – from the moment they are sent from the source device to the moment they are received by the destination device. Therefore, it also covers the interception of electronic communications data that are temporarily stored during the process of transmission.

The electronic communications data, which are stored before or after the process of transmission (e.g., e-mail drafts or sent e-mails, e-mails stored by the provider, received e-mails stored by the recipient, or completely web-based communication such as in social networks), are not protected by telecommunication secrecy but are recognized as documents stored in private, which means that access to such data is covered by different provisions Code of Criminal Procedure (see below).

bb) Access after the end of telecommunication transmission

Since the Code of Criminal Procedure is rather old, it does not deal with access to data or stored electronic communications in detail. The only detailed rules are related to access to the traffic data retained by electronic communications service providers.[91] Apart from that, there are no specific provisions providing clear rules for accessing the communication data. Therefore, if there is a need to access communication data, the law enforcement authorities are forced to apply more general rules, which were originally made for different purposes.

Methods usually used to access electronic communications data stored before the beginning or after the end of telecommunication transmission (message drafts, sent messages, stored received messages, etc.) vary, depending on the source of such data.

The communication data may be stored in a device (hard drives, flash drives, mobile phones, computers, etc.), which may be acquired following provisions on

---

[91] Section 88a Code of Criminal Procedure.

the obligation to present assets,[92] or the seizure of assets,[93] seized during house or personal searches,[94] or examined.[95] Such communication data can be accessed without further consent from the judge or Public Prosecutor. There is also discussion on which data are considered to be stored in the seized computer system. For example, according to some interpretations, even communication data that are stored in connected[96] cloud storage may be accessed from the seized device without further consent, because it is considered a part of such computer system. There is, however, no official opinion or judicial decision that would clarify this matter.

If the data is stored elsewhere (by the provider, in the cloud, in someone else's device, etc.), then it is protected as records stored in private and may be accessed only with prior consent of a judge (surveillance of persons or items[97]) or prior consent of the respective user. This approach is also supported by Opinion No. 1/2015 of the Supreme Public Prosecutor's Office, which states (informal translation[98]):

> "The current content of the e-mail inbox is determined by the will of the user and can be accessed following the rules stipulated in section 158d para. 3 Code of Criminal Procedure, which can be considered a legal license to overcome the constitutional right to privacy of records located in e-mail inbox […]."

However, this applies only to the data stored in the device or on the server at the moment of seizure or first access. Should the seized device or obtained access be further used for interception of transmission received in the future, an order for the interception and recording of telecommunication is necessary. This is also supported by the above-cited opinion, which states in para. 3 (informal translation):

> "Access to the e-mail communication in real time is possible only following the rules specified in section 88 para. 1 Code of Criminal Procedure, because, like the telecommunications traffic, it also takes place in an electronic communications network."

The government is aware of the obsolescence Code of Criminal Procedure and is therefore preparing its complete recodification. As far as the national rapporteur knows, during the preparation of the recodification, the possibility of introducing specific provisions for access to electronic data, including communication data, is also being discussed. However, the entire process of recodification is in

---

92 Section 78 Code of Criminal Procedure.

93 Section 79 Code of Criminal Procedure.

94 Section 82 Code of Criminal Procedure.

95 Section 113 Code of Criminal Procedure.

96 Connected cloud storage means a situation when the seized device is actively using a cloud storage service, which still synchronizes with the device files stored in the cloud after the device is seized.

97 Section 158d Code of Criminal Procedure.

98 Opinion No. 1/2015 of the Supreme Public Prosecutors Office on the harmonization of interpretation of laws dealing with access to mobile devices and other storage media, including the content of e-mail inboxes. This document is not available in English, translation by the national rapporteur.

its infancy, and so we cannot expect any substantial changes in the legislation in the near future.

3. Special protection of confidential communication content

The main provision provides protection only for the communication between the defence counsel and the accused. Such a communication is inadmissible in criminal proceedings and, if the police authorities find during the interception that the accused has communicated with his/her defence counsel, they are obliged to immediately destroy the interception recording and not use the information learned in this context in any way.[99] These rules are deemed rather problematic by some sources. The reason is that most interceptions are conducted before the commencement of the criminal prosecution and, in this stage, the person against whom the criminal proceedings are being conducted is not referred to as the accused. Therefore, *stricto sensu* interpretation of the provision would mean that, before the commencement of criminal prosecution, the police would be able access and use even the communication between the person against whom the criminal proceedings are being conducted and his/her attorney. Some sources see this as an intrusion into the right to a fair trial.[100]

However, the protection of the communication between the defence counsel and the accused is not absolute. Particularly when the communication relates to a crime, which is committed by the defence counsel in cooperation with the accused, then the protection does not apply. This approach is even supported in the Decision of Constitutional Court No. I.ÚS 1638/14, which states (informal translation[101]):

> […] However, as is clear from the case law of the European Court of Human Rights and of the Supreme Court, the protection of communication between solicitor and his client is not absolute, inviolable and under certain circumstances may be limited. Possible criminal activity of the solicitor, both to the detriment of the client or to the detriment of others in complicity with the client, can't be considered as the provision of legal services, and in such a case it is impossible to provide any protection of such activity. […]

4. Execution of telecommunication interception

The criminal law does not specify which modes of interception law enforcement authorities should use. According to Act No. 237/2008 Sb. on the Police of the

---

[99] Section 88 para. 1 Code of Criminal Procedure.

[100] For example, in Czech, see *Vantuch, P.*, Nová úprava odposlechu v trestním řádu od 1.7.2008. Bulletin advokacie, 2008, no. 10, p. 29.

[101] Decision No. I. ÚS 1638/14. Available online in Czech at http://nalus.usoud.cz/Search/GetText.aspx?sz=1-1638-14_1. Provided excerpt translated by the national rapporteur.

Czech Republic, these activities are conducted by the Czech police (informal translation[102]):

> **Section 19 Police Act**
>
> The police can technically provide the use of intelligence technologies or bait and security techniques or surveillance of persons and items at the request of the national authority, which is authorised for such use.
>
> State authority shall demonstrate in the request, that the use of intelligence technologies or surveillance of persons and items is allowed according to other legislation.

A special police unit called Unit for Special Activities is responsible for the interception. The Unit for Special Activities is a specialized unit, which, in accordance with the Code of Criminal Procedure, the Act on the Police of the Czech Republic, and other relevant legislation, carries out interception and recording of telecommunication traffic and surveillance of persons and items for authorized security bodies. It is the only unit authorized to carry out these operations and this position is reflected in its organizational structure – its headquarters are located in Prague and it has subsidiaries in each region of the Czech Republic. Every interception order is forwarded to this unit, which subsequently carries out the interception. The recordings of intercepted traffic are then provided to the investigator who is responsible for the respective criminal prosecution.

The specific methods they use are classified, but, as far as the national rapporteur knows, the police usually intercept the communication using dedicated access points, which ISPs are obliged to install into their infrastructures.[103] They can probably also intercept the communication without any recourse to third parties (ISPs) using special equipment and tools, even though it is not very common. Also, if practical, the police may also order the ISP to extract and surrender specific stored communication data.

There are no accompanying investigative measures mentioned in the main provision itself. Law enforcement authorities may, however, follow different provisions in order to access houses or other places[104] or to be able to use specific technical measures to gain access to the communication.[105]

5. Duties of telecommunication service providers to cooperate

a) Possible addressees of duties of cooperation

There is no specific provision requiring ISPs to execute interception orders themselves. However, any natural or legal person is required to comply with letters

---

[102] Act No. 237/2008 Sb. on the Police of the Czech Republic. This act is not available in English, translation provided by the national rapporteur.

[103] See Section 97 of Act No. 127/2005 Sb. on electronic communications.

[104] See Section 82 Code of Criminal Procedure.

[105] See Section 158d Code of Criminal Procedure.

of request from law enforcement authorities for the performance of their actions according to Section 8 Code of Criminal Procedure (informal translation[106]):

Section 8 Code of Criminal Procedure

(1) Public authorities, legal entities and natural persons are required to comply with letters of request from law enforcement authorities for the performance of their actions without undue delay and unless a special regulation stipulates otherwise, to comply without payment. Furthermore, public authorities are also obliged to immediately notify the public prosecutor or the police authorities of facts indicating that a criminal offence has been committed.

Hence, if the interception can only be done by ISPs in specific cases, then they are required to execute the order.

As far as the national rapporteur knows, classified agreements between the Unit for Special Activities and some ISPs exist (especially on the IP-application level – social networks, cloud providers, etc.), which simplify such cooperation.

Additionally, the Act on Electronic Communications obliges entities providing a public communications network or publicly available electronic communications service to install specific equipment for interception in their infrastructures and to cooperate during an interception (see below). These entities are defined in the following provisions (informal translation[107]):

Section 2 Act on Electronic Communications – Definitions

For the Purposes of this Act

[…]

f) "provision of an electronic communications network" means the establishment, operation or supervision of such a network, or making it accessible,

[…]

h) "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other facilities, including network elements which are inactive and which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed circuit-switched or packet-switched networks and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting and cable television networks, irrespective of the type of information conveyed,

[…]

j) "public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services, and which supports the transfer of information between network termination points, or an electronic communications network through which a service distributing radio and television broadcasts is provided,

[…]

---

[106] See Section 8 Code of Criminal Procedure, cited below.

[107] Act No. 127/2005 Sb., English translation available online at http://www.mpo.cz/dokument156553.html

n) "electronic communications services" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, and on cable television networks, but excluding services that offer content by means of electronic communications networks and services, or exercise editorial control over the offered content transmitted using electronic communications networks and services; it does not include information society services, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks,

o) "publicly available electronic communications service" means an electronic communications service from the use of which no person is excluded beforehand,

[…]

It is important to note that these obligations apply only to the aforementioned providers of a network infrastructure or electronic communications service, which are licensed by the Czech Telecommunications Office. However, providers of services of information society services[108] (IP-application level – Internet applications, cloud, e-mail services, social networks, etc.) are not specifically obliged to provide such cooperation.

b) Content of duties to cooperate

According to Section 97 of Act No. 127/2005 Sb. on electronic communications, the entity providing a public communications network (infrastructure providers working at the IP-transport level) or publicly available electronic communications service (access providers at the IP-transport level) is required to allow interception and recording of transferred communication at the expense of the police. Relevant parts of the above-mentioned provision are cited below (informal translation[109]):

Section 97 Act on Electronic Communications

(1) A legal entity or natural person providing a public communications network or a publicly available electronic communications service shall, at the expense of the requesting party, provide and secure interfaces at specified points of the network to connect terminal equipment for message tapping and recording:

a) for the Police of the Czech Republic for the purposes specified in a special legal regulation[36]),

[…]

(2) The bodies listed in Subsection 1 above shall prove their authorisation for message tapping and recording by submitting a written application, which contains a reference number under which the court ruling is filed by this body, and which is signed by the person responsible from the body listed in Subsection 1 above for the performance of the message tapping and recording. In the event of message tapping and recording by the Police of the Czech Republic in accordance with special legal regulations[36]) the written application shall contain a reference number under which the consent of the user of the station monitored is filed by the Police of the Czech Republic.

---

[108] According to Act No. 480/2004 Sb. on some services of the information society.

[109] Act No. 127/2005 Sb., English translation available online at http://www.mpo.cz/dokument156553.html

[…]

(3) A legal entity or natural person providing a publicly available telephone service is required, on request, to provide information from the database of all its subscribers to the publicly available telephone service to a body authorised to request them in accordance with a special legal regulation, at their own expense. The form and scope of the information provided is stipulated in an implementing legal regulation.

(4) Where a legal entity or natural person providing a public communications network or a publicly available electronic communications service introduces into its activities any coding, compression, encryption or any other method of transmission that makes the messages being transmitted incomprehensible, such a person shall ensure that the messages requested and the traffic and location data related thereto are provided in a comprehensible manner at the termination points for connection of the terminal equipment referred to in Subsection 1 above.

(5) For fulfilling the obligations specified in Subsections 1, 3 and 5 above, the legal entity or natural person is entitled to reimbursement for effectively incurred costs from the authorised body which requested or ordered such an action. The amount and method of reimbursement for the effectively incurred costs is set out in an implementing legal regulation.

(6) A person referred to in Subsection 1 above and its employees are required to maintain the confidentiality of any tapping or recording of messages requested or implemented in accordance with Subsections 1 and 2 and data requested or provided in accordance with Subsections 3 and 5 and matters related thereto.

(7) The technical and operational conditions and points for the connection of terminal telecommunications equipment for the tapping or recording of messages is set out in an implementing legal regulation.

(8) A legal entity or natural person providing a public communications network or a publicly available electronic communications service shall keep records on:

a) the number of cases where, on requested, it provided traffic and location data to the bodies authorised to request them,
b) the period that elapsed, in each case, from the date on which the storage of the traffic and location data began to the date on which the authorised body requested such data, and
c) the number of cases when it was not able to comply with a request to provide traffic and location data.

(9) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service is required to provide to the Office the collective records referred to in Subsection 10 above, for the previous calendar, in electronic form, at the latest by 31 January of the following calendar year. The records provided may not contain personal and identification data. The Office shall immediately send the collective records received to the Commission.

(10) The form of the records provided under Subsection 11 and the method of their submission to the Office is stipulated in an implementing legal regulation.

According to this provision, these providers are required to install a dedicated interface in their infrastructures, which the Unit for Special Activities can use to connect its devices to access ongoing traffic.

c) Duties to provide technical infrastructure

Communication providers are required to follow rules on interception capabilities in their networks, specified in Decree No. 336/2005 Sb. In accordance with this decree, providers and the police shall agree on the technical parameters of the equipment, which the provider will purchase and install into the network or service in order to provide an interface to connect devices for wiretapping (informal translation[110]):

Section 7 Decree No. 336/2005

(1) A legal entity or natural person providing a public communications network or a publicly available electronic communications service shall (hereinafter "operator") shall equip its network or service with interface for connecting devices for interception on the basis of the request from competent authority.

(2) If the operator is developing a new network or service, expanding or changing significantly existing network or service, he shall prompt competent authority to issue a request for equipping the network or service with interface for connecting interception devices. The competent authority shall issue the request within 15 days from prompting.

(3) On the basis of request issued according to the paragraph 1 or 2, the operator in cooperation with the competent authority shall propose possible technical solutions, including the reasons for their implementation and calculation of cost of each solution.

(4) Chosen solution and its parameters shall be specified in a record jointly elaborated by the competent authority and the operator. The record shall also include calculation of financial cost and method and schedule of the payment.

d) Security requirements for data transfers by communication service providers

According to Section 13 of Decree No. 336/2005 Sb., the intercepted communication is transferred to the police via hard data link or via secure virtual channel on the Internet (using the standardized communication protocol SFTP – the provider accesses the police server). The data provided should be equipped with a specific identifier and a time-stamp. The integrity of the data is to be ensured by creating a fingerprint using the SHA-1 hash function. Intercepted e-mails may also be sent to the police via dedicated SMTP server. There are no specific rules for the transfer of the intercepted data to authorities in a foreign country. The respective provision states the following (informal translation[111]):

---

[110] Decree No. 336/2005 Sb. on technical and operational conditions and points of connection of the telecommunications equipment for interception and recording of telecommunications traffic. This decree is not available in English to date. Cited provision translated by the national rapporteur.

[111] Section 13 of Decree No. 336/2005 Sb. on technical and operational conditions and points of connection of the telecommunications equipment for interception and recording of telecommunications traffic. This decree is not available in English to date. Cited provision translated by the national rapporteur.

Section 13 Decree No. 336/2005 – Packet Networks Outputs

(1) The output of the network or service is provided via

a) hard data link, or

b) secure virtual channel on the Internet using standardized communication protocol FTP, server shall be provided by competent authority and operator should connect as a client.

(2) Sent data unit shall be equipped with identifier of user address and serial number or time stamp. Data integrity of the data unit shall be ensured by creation of file stamp using hash function SHA-1.

(3) During the interception of e-mails, may the operator, with consent from the competent authority, send copies of messages using protocol for transferring e-mail to the SMTP server provided by the competent authority.

e) Checks, filtering, and decryption obligations of communication service providers

As far as the national rapporteur is aware, no checks and filtering obligations for Internet providers are mentioned in the statutory law. ISPs (providers of a public communications network or a publicly available electronic communications service) are, however, according to Section 97 Act on Electronic Communications, obliged to provide access to decrypted traffic if they are using any form of encryption (informal translation[112]):

Section 97 Act on Electronic Communications – Tapping and recording messages

[…]

(4) Where a legal entity or natural person providing a public communications network or a publicly available electronic communications service introduces into its activities any coding, compression, encryption or any other method of transmission that makes the messages being transmitted incomprehensible, such a person shall ensure that the messages requested and the traffic and location data related thereto are provided in a comprehensible manner at the termination points for connection of the terminal equipment referred to in Subsection 1 above.

If the communication is encrypted by the user or by the provider of IP-application level services, then the ISP is not obliged to assist the competent authorities in decrypting such encryption in any way. Also, these rules do not apply in case of providers of information society services (IP-application level); however, they may be required by the police authority performing surveillance in order to provide access to decrypted communication data, if it is necessary for successful surveillance of persons and items, according to Section 158d para. 9 Code of Criminal Procedure (informal translation[113]):

---

[112] Act No. 127/2005 Sb., English translation available online at http://www.mpo.cz/dokument156553.html.

[113] Act No. 141/1961 Sb. on criminal procedure. Translation taken from the legal information system ASPI.

Section 158d Code of Criminal Procedure – Surveillance of persons and items

[…]

9) Operators of telecommunications activity, their employees, and other persons who participate in the operation of telecommunications activity, as well as the post office or the person performing the transport of the consignments are obligated to provide the police authority performing the surveillance with the necessary assistance free of charge and in accordance with their instructions. At the same time, they may not claim the obligation of professional confidentiality imposed by special Acts.

6. Formal prerequisites of interception orders

a) Competent authorities

The interception of electronic communications may be conducted only after the interception order is issued. The interception order is a decision *sui generis.*

Only the Public Prosecutor can apply for the interception order in preliminary proceedings, usually after consultation with the police investigator. Prior to submitting the application, the Public Prosecutor usually verifies whether the criminal proceedings are being conducted for a crime for which the interception can be ordered. He particularly assesses whether the offense described in the record of the commencement of the criminal proceedings or in the resolution to initiate the criminal prosecution corresponds with legal classification used. He also assesses whether it may be reasonably assumed that facts relevant to the criminal proceedings will be obtained during the interception if there is no other way to achieve such purpose or if its achievement would otherwise be significantly reduced.

Justified application is then presented to the judge, who can authorize the interception by issuing the order according to Section 88 para. 2 Code of Criminal Procedure (informal translation):

Section 88 Code of Criminal Procedure – Interception and recording of telecommunications

[…]

(2) The presiding judge and, in preliminary proceedings upon the petition of the public prosecutor, the judge, is entitled to warrant the interception and recording of telecommunications. […] The order for the interception and recording of telecommunications shall immediately be forwarded to the police authority. In the preliminary hearing, the judge shall send a copy of the order for the interception and recording of telecommunications to the public prosecutor without undue delay.

This procedure is described in detail in Section 32 of the instruction of the Ministry of Justice Ref. No. 505/2001-Org, which issues the internal and office directives for courts (informal translation[114]):

---

[114] Instruction of the Ministry of Justice Ref. No. 505/2001-Org, which issues the internal and office directives for courts. Provision translated by the national rapporteur.

Section 32 Interception and recording of telecommunications

(1) The judge shall, at the time of reachability, apply procedure described in section 27 para. 1.

(2) The judge shall decide on the application of the public prosecutor for interception and recording of telecommunications traffic in accordance with section 88 para. 2 Code of Criminal Procedure (hereinafter "interception") without delay or within the period agreed with the public prosecutor; on the proposal of the public prosecutor to extend duration of the interception (section 88 para. 4 Code of Criminal Procedure) will the judge decide no later than the last working day before the expiry of the previously issued interception order, if the public prosecutor filed the proposal at least 3 working days before expiry of the interception order.

The order is then forwarded to the investigator and to the Unit for Special Activities, which carries out the interception.

These rules apply even in the case of any type of emergency.

b) Formal requirements for applications

There are no specific requirements for applications but, according to Art. 67 of the binding Guideline of the Police President No. 30/2009 Sb. on the tasks in criminal proceedings,[115] an application usually contains the following information:

- the identifier of the device or the user, if his identity is known;
- specific facts about the case, which justify the need to issue the interception order and its duration;
- if the criminal proceedings are being conducted for an intentional criminal offense for which prosecution is stipulated in a declared international treaty, a reference to this treaty;
- a description of the offense and its legal classification;
- a list of interception orders already issued for the same identifier;
- the application for an interception order itself.

The complexity of justification and description of the case in individual applications varies, depending on the complexity of each case. The application may also be submitted with investigative files or other additional materials. Applications are submitted to the court in written form.

c) Formal requirements for orders

Basic formal requirements for interception orders are defined in Section 88 para. 2 Code of Criminal Procedure as follows (informal translation):

---

[115] Binding Guideline of the Police President No. 30/2009 Sb. on the tasks in criminal proceedings. Available online in Czech at http://www.pecina.cz/files/pokyn2.pdf

Section 88 Code of Criminal Procedure

[…]

(2) The order for the interception and recording of the telecommunications service shall include a determined user address or a user device and the user if their identity is known, and the justification of the order must include the specific facts that justify the issue of such order as well as its period. […]

The Constitutional Court in its Decision No. II. ÚS 615/06[116] also dealt with formal requirements of interception orders. According to the Decision, the interception order must be supported by relevant evidence from which we can derive reasonable suspicion of committing a crime. The mere existence of criminal complaint is not sufficient justification for issuing the interception order. In addition, the court stated that the interception order must be individualized in relation to a specific person or device. It must also specifically state which facts relevant to the criminal proceedings will probably be obtained. The court criticized the practice of issuing some interception orders even though the material conditions of the case had not been sufficiently assessed. Hence, the interception order also must contain an assessment of these conditions.

Based on these findings, the interception order should contain at least the following:

– the interception order;
– identifier of the user or the device;
– the name of the user, if known (name, address, etc.);
– the identification of the crime for which the criminal proceedings are being conducted (reference to international treaty if applicable);
– the duration of the interception (no longer than four months).

Additionally, the justification of the order should contain:

– specific facts about the case, which justify issuance of the interception order and its duration;
– the purpose of the interception;
– an explanation of the reasons why there is no other way to achieve such purpose or why its achievement would otherwise be significantly reduced.

7. Substantive prerequisites of interception orders

a) Degree of suspicion

Required degree of suspicion is not specified in the positive law, but it usually is evaluated on the case by case basis by the judge. In some interception orders judges

[116] Decision No. II. ÚS 615/06. Available online in Czech at http://nalus.usoud.cz/Search/GetText.aspx?sz=2-615-06_1

did not assess the degree of suspicion enough, so the Constitutional Court stated in the above-cited decision, that the order should contain at least relevant clues from which we can derive reasonable suspicion of committing required crime.

b) Predicate offences

According to Section 88 para. 1 Code of Criminal Procedure, the interception order can be justified by following crimes:

- machinations in insolvency proceedings;
- violation of regulations on rules of competition;
- negotiating advantages during public procurement, tenders, and auctions;
- machinations during public procurement and tenders;
- machinations at a public auction;
- misuse of powers by an official person;
- other intentional criminal offenses for which prosecution is stipulated in a declared international treaty.

Additionally, the interception order can be justified in case of crimes for which the law stipulates the upper value of the prison sentence range as at least eight years.

c) Persons and connections under surveillance

As far as the national rapporteur is aware, anyone and any device that fall within the scope of Act on Electronic Communications may be subject to an interception order if the required criteria are met and if the judge considers the reasoning of the application sufficient. According to Section 2 Act on Electronic Communications, the user is defined as "anyone who uses or requests a publicly available electronic communications service;" thus it includes users of IP-transport level services as well as users of IP-application level services.

Since the interception order has to include a determined user address or user device, it cannot target specific communication content but only a particular person.

There is also debate over whether the interception order also covers transmission outside of the network. In a recent decision, it was mentioned that the interception record also contained conversation which took place near the phone, at the moment connection was being established to another phone.[117] According to technicians, the phone transmits surrounding sounds even before the other party to the call picks up the phone and, according to the above-mentioned decision, even these sounds

---

[117] Page 50 of the decision of the city court in Prague of 30 April 2014 no. 42 T 8/2013. Available in Czech at http://www.pecina.cz/files/Rozsudek_MS-P_30.4.2014.pdf

are part of the interception record. Use of such a record as evidence is rather problematic, because nobody can reasonably expect that the phone transmits surrounding sounds to the provider even before the call itself begins. There is, however, no case law at the moment that would clarify this matter.

d) Principle of subsidiarity

The order for the interception and recording of telecommunication may be issued if it can be reasonably assumed that facts relevant to the criminal proceedings will be obtained in this way and if there is no other way to achieve said purpose or if its achievement would otherwise be significantly reduced.[118] The investigator, the Public Prosecutor and, most importantly, the judge should therefore consider whether the specific facts relevant for criminal proceedings could be secured by other less intrusive means of investigation referred to in the Code of Criminal Procedure.

This approach is based upon basic principles of criminal proceedings defined in Section 2 Code of Criminal Procedure, especially the principle of proportionality and the principle of moderation formulated in Section 2 para. 4 as follows (informal translation):

Section 2 Code of Criminal Procedure

[…]

(4) Criminal cases shall be dealt with with a full investigation of rights and freedoms guaranteed by the Charter of Fundamental Rights and Freedoms and by international treaties on human rights and fundamental freedoms that the Czech Republic is bound by; when conducting acts of criminal proceedings, the rights of persons that such acts affect may be intervened only when justified by law and to the extent necessary to ensure the purpose of criminal proceedings. […]

e) Proportionality of interception in individual cases

There is no additional obligation for the authorizing authority to verify that the interception is proportionate to the seriousness of the offense in an individual case. The proportionality is, however, always assessed in the interception order. For example, if the police authority were to apply for too many interception orders in one case, the judge would probably refuse to issue it, because he would find it disproportionate and against the principle of moderation formulated in the above-cited Section 2 para. 4 Code of Criminal Procedure.

f) Consent of a communication participant to the measure

If the user of the intercepted unit agrees to such a measure, the law enforcement authority may order the provider to intercept and record telecommunication or con-

---

[118] Section 88 para. 1 Code of Criminal Procedure.

duct it himself, even without the order for the interception and recording of telecommunication, but only if there is a criminal proceeding for following criminal offenses:

– human trafficking;
– the delegation of custody of a child to someone else;
– restriction of personal freedoms;
– extortion;
– kidnapping of a child and persons suffering from a mental disorder;
– violence against a group of people or an individual;
– dangerous threats;
– dangerous persecution.[119]

This provision is criticized by some, because it infringes the telecommunication secrecy of intercepted user who did not provide the consent. Normally, such infringement is justified on the basis of a proper court order, in which the judge assesses whether there is a reasonable reason for interception; in this case, however, the protection is somewhat weaker. Yet, some kind of protection is provided according to the General Instruction of the Supreme Public Prosecutor No. 8/2009 on criminal proceedings, which states in Section 45 (informal translation[120]):

> **Section 45 Interception without court order**
>
> Public prosecutor shall make sure, that if police authority order interception and recording of telecommunication without court order, it shall inform him immediately. The public prosecutor then assesses whether the interception was ordered in the criminal proceedings for the offence for which it is possible to use this measure, and that throughout the period of interception such qualification is justified. If the public prosecutor considers, that the interception could not lead to obtaining of facts important for the criminal proceedings, or that the consent is invalid or was waived, he orders the police authority to immediately discontinue the interception and destroy obtained records. Obtained information can't be in this case further used. If the interception is ordered by the public prosecutor, the provisions on the interception ordered by the judge shall adequately apply.

8. Validity of interception order

a) Maximum length of interception order

The maximum length of an interception order is four months.

---

[119] Section 88 para. 5 Code of Criminal Procedure.

[120] General Instruction of the Supreme Public Prosecutor No. 8/2009 on criminal proceedings. Cited provision translated by the national rapporteur.

b) Prolongation of authorization

Based on the assessment of the ongoing course of the interception, the judge of a superior court and, in a preliminary hearing upon petition of the Public Prosecutor, a deputy county court judge may even extend the duration of the interception and recording of telecommunication traffic repeatedly, however always only for a maximum period of four months.

c) Revocation of authorization

There is no positive provision that would deal with possibility of revocation of the interception order. In the opinion of the national rapporteur, however, the issuing judge may decide to revoke the order when a lack of substantive prerequisites for the interception becomes apparent. The Constitutional Court may also revoke the interception order.

According to Section 88 para. 8 Code of Criminal Procedure, the Supreme Court may subsequently review the legality of the interception order, following the procedure described in Sections 314l–314n Code of Criminal Procedure (informal translation):

§ 314l Code of Criminal Procedure

(1) Upon the petition of the person referred to in Section 88 Subsection 8, the Supreme Court, in closed hearing, shall examine the legality of the warrant for the interception and recording of the telecommunications service.

(2) Upon the petition of the person referred to in Section 88a Subsection 2, the Supreme Court, in closed hearing, shall examine the legality of the order for the ascertainment of data on the telecommunications service.

§ 314m Code of Criminal Procedure

(1) If the Supreme Court finds that the warrant for the interception and recording of the telecommunications service or the order for the ascertainment of data on the telecommunications service was issued or its performance was contrary to law, they shall pronounce the violation of the law by a resolution.

(2) An appeal against such decision is not permissible.

§ 314n Code of Criminal Procedure

(1) If the Supreme Court finds that the warrant for the interception and recording of the telecommunications service was issued and its performance was in compliance with the conditions set out in Section 88 Subsection 1 or the order for the ascertainment of data on the telecommunications service was issued and its performance was in compliance with the conditions set out in Section 88a Subsection 1, they shall pronounce in a resolution that the law was not violated.

(2) An appeal against such decision is not permissible.

The police authority is also obliged to continuously assess whether the reasons that led to an order for the interception and recording of telecommunication are still valid. If the reasons are no longer valied, the police are obligated to immediately

terminate the interception and recording of telecommunication, even before the end of the period for which the interception order was issued. The judge who issued the order for the interception and recording of telecommunication must also be immediately informed in writing.[121]

9. Duties to record, report, and destroy

a) Duty to record and report

Intercepted data and communication are securely stored by the Unit for Special Activities and provided to the police investigator. He then assesses the content of the data and prepares the interception record – a document that usually contains transcripts of parts of the communication relevant to the criminal proceedings. If the record is to be used as evidence in the criminal proceedings, it needs to be accompanied by a protocol. According to Section 88 para. 6 Code of Criminal Procedure, the protocol must contain information on the place where the interception was conducted, time of interception, manner of interception, authority who issued the recording, and general information on contents of the record. The protocol must also contain general information required by Section 55 Code of Criminal Procedure as follows (informal translation):

Section 55 Code of Criminal Procedure – General provisions for transcript recording

(1) Unless the law stipulates otherwise, at any action of criminal proceedings a transcript is recorded, usually during an action or immediately after, which must include

a) the name of the court, public prosecutor or other law enforcement authority,
b) the place, time and subject of an action,
c) name and surname of officials and their functions, name and surname of the parties present, the name, surname and address of the legal representatives, legal counsel and agents who participated in the action, and in the case of the victim and the accused also the address that is specified for the purpose of delivery, and other data necessary to establish or verify identities, including date of birth or birth certificate numbers,
d) brief and concise statements of the course of an action which would be seen as preserving the statutory provisions governing the conduct of an action, essential contents of the decisions announced during an action, and if a copy of the decision was delivered immediately after reaching the decision, and the confirmation of this service; if there is a literal transcript of the person's statement, it is necessary to indicate such in the transcript accordingly so that it is possible to safely identify the beginning and end of the literal transcript,
e) petitions of the parties, issued instructions, and/or an expression of the instructed persons,
f) objections of the parties or the persons interviewed during the execution of an action or the content of the transcript.

---

[121] Section 88 para. 3 Code of Criminal Procedure.

(2) Should the identified condition indicate that the witness or persons close to them appear to be under threat of bodily harm or any other serious risk of violation of their fundamental rights in relation to their testimony and witness protection can not be safely ensured by some other means, the law enforcement authorities shall take steps to conceal the identity of the witness; the name and surname and other personal information is not recorded in the transcript but are kept separate from the criminal file and only law enforcement authorities may gain access to such details for the purpose of the case. A witness shall be instructed on the right to request confidentiality of their identity and must sign the transcript under an assumed name and surname under which they are further recorded. If the protection of such persons is required, law enforcement authorities must take all necessary steps without undue delay. A special manner to protect witnesses and persons close to them is stipulated by a special Act. If the reasons for the confidentiality of identity and a separate record of personal data of witnesses has expired, the authority responsible for the legal proceedings at the time shall revoke the level of classification of information, attach the information to the criminal file, and the identity and details of the witnesses cease to be classified; this does not apply to the classified identity of persons listed in Section 102a.

(3) The transcript drawn up on the conflict shall include literal testimonies of the confronted persons, as well as the wording of questions and answers; and the circumstances that are important in terms of the purpose and implementation of the confrontation. The transcript is drawn up about the recognition and it must include detailed circumstances under which the recognition was performed, in particular the order in which the persons or items are shown to the suspect, accused or witness, the time and conditions of their observations and their opinions; the recognition conducted in the preliminary hearing is usually video recorded. The transcript drawn up about the investigative attempt, the reconstruction and on-site review is necessary to describe all the circumstances under which these actions were carried out in detail, including their contents and results; if the circumstances of the case do not exclude it, video recordings, sketches, and other appropriate tools shall, if possible, be included in the transcript. Similarly, it is necessary to proceed even if an event when the implementation of other evidence is not explicitly provided by law.

(4) The transcript in the Czech language is drawn up on the testimony of a person even if the questioned person speaks another language; depending on the literal testimony, the reporter or an interpreter shall record the relevant part of the testimonies in the language spoken by the person who testifies.

(5) The correct transcript is guaranteed by the person who performs the operation.

The police authority is not obliged to provide any reports on the progress of the interception or any other final report to the judge. The record is, however, available to the Public Prosecutor, who should regularly assess its content and the legality of the interception.

b) Duty to destroy

If the interception did not uncover any facts relevant to the criminal proceedings, the police authority, after approval by a court and, in preliminary hearings, the Public Prosecutor, must immediately destroy all records three years after the matter has been concluded.[122]

---

[122] Section 88 para. 7 Code of Criminal Procedure.

If the police authority was informed of an extraordinary appeal within the set deadline, the records of the interception shall be destroyed after the decision on the extraordinary appeal has been taken or after the matter has been concluded.

The police authority is responsible for the destruction of the record and a transcript of the destruction of the record of the interception must also be sent to the Public Prosecutor, whose final decision concluded the matter. In proceedings before the court, the destruction transcript must be sent to the presiding judge in the first instance, for the record on file. The police authority also orders the Unit for Special Activities to destroy their respective records.

Also, if the police authority finds that the accused has communicated with his/her defence counsel during the interception and recording of telecommunication, the respective part of the interception recording must be destroyed immediately. In this case, the report on the destruction of the record is to be placed in the file.[123]

10. Notification duties and remedies

a) Duty to notify persons affected by the measure

The Public Prosecutor or the police authority, upon whose decision the case was finally concluded, and, in proceedings before the court, the presiding judge in the first instance after the final conclusion of the matter, shall inform the affected person, if known, about the ordered interception and recording of telecommunication service.[124] The information should include the designation of the court that issued an order for the interception and recording of telecommunication service, the duration of the interception, and the date of the conclusion.

The information about the interception is not provided to the affected person in the following cases:

– when criminal proceedings are conducted for specific crimes;
– when the criminal offense has involved several people and the criminal proceedings have not yet been concluded in relation to at least one of them;
– when it could lead to threats to national security, life, health, or the rights and freedoms of individuals, etc.[125]

b) Remedies

The affected person may file a petition to review the legality of the order for the interception and recording of telecommunication services with the Supreme

---

123 Section 88 para. 1 Code of Criminal Procedure.

124 Section 88 para. 8 Code of Criminal Procedure.

125 See Section 88 para. 9 Code of Criminal Procedure.

Court.[126] The procedure of judicial review is described in provisions 314l–314n Code of Criminal Procedure (cited *supra* in II.B.8.a.)

c) Criminal consequences of unlawful interception measures

The officials conducting interceptions illegally may be held liable for the criminal offense of violating the confidentiality of messages according to Section 182 Penal Code (informal translation[127]):

Section 182 Penal Code – Violating confidentiality of messages

(1) Whoever intentionally violates the confidentiality

a) of a closed letter or other document during the provision of postal services or transported by other transport services or transport facilities,

b) of data, text, voice, audio or video messages sent via electronic communications networks and attributable to an identified subscriber or user who receives the message, or

c) of non-public transmission of computer data into a computer system, from or within which, including electromagnetic radiation from a computer system, transferring such computer data,

shall be punished by a prison sentence of up to two years or punishment by disqualification.

(2) Whoever with the intention to cause damage to another person or to procure an unauthorised benefit for themselves or another person

a) reveals the secret of which they learned from the document, telegram, telephone call or electronic transmission through a communications network, which was not intended for them , or

b) takes advantage of such secrets, shall be similarly punished.

(3) An offender shall be punished by a prison sentence of six months to three years or punishment by disqualification, if

a) they committed an act referred to in Subsection 1 or 2 as a member of an organised group,

b) they committed such an act out of reprehensible motives,

c) they caused substantial damage by committing such an ac, or

d) they committed such an act with the intention of gaining a substantial benefit for themselves or someone else.

(4) An offender shall be punished by a prison sentence of one to five years or a monetary penalty, if

a) they committed an act referred to in Subsection 1 or 2 as an official person,

b) they caused large-scale damage by committing such an act, or

c) they committed such an act with the intention to procure another large-scale benefit for themselves or someone else.

---

126 Section 88 para. 8 Code of Criminal Procedure.

127 Act No. 40/2009 Sb., Penal Code. Translation taken from the legal information system ASPI.

They and also the judge who issues illegal interception order may be held liable for the criminal offense of abuse of powers by an official according to Section 329 Penal Code (informal translation):

Section 329 Penal Code – Abuse of powers of an official person

(1) An official person who, with the intention to cause damage or other serious harm to another person or to procure an unauthorised benefit for themselves or another person

a) performs their powers in a manner contrary to another legal regulation,

b) exceeds their powers, or

c) fails to meet an obligation under their powers,

shall be punished by a prison sentence of one to five years or punishment by disqualification.

(2) An offender shall be punished by a prison sentence of three to ten years, if

a) they procured a substantial benefit for themselves or another person by committing an act referred to in Subsection 1,

b) they committed such an act on another person for their actual or perceived race, ethnicity, nationality, political belief, religion, or because they are actually or allegedly non-religious,

c) they caused substantial disruption to the activities of a public administration body, local government, court or another public authority by committing such an act,

d) they caused serious disruption to the activities of a legal entity or natural person who is an entrepreneur by committing such an act,

e) they committed such an act while abusing the vulnerability, addiction, anxiety, cognitive weakness, or inexperience of another person, or

f) they caused substantial damage by committing such an act.

(3) An offender shall be punished by a prison sentence of five to twelve years or forfeiture of property, if

a) they procured another large-scale benefit for themselves or another person by committing an act referred to in Subsection 1, or

b) they caused large-scale damage by committing such an act.

(4) Premeditation is punishable.

A Parliamentary Commission to monitor the use of interception and recording of telecommunication traffic controls the interception of communication according to Section 98 of the Act on the Police of the Czech Republic as follows (informal translation[128]):

Section 98 Police Act

Supervision of the use of interception and recording of telecommunications, use of surevillance of persons and items and interference with the operation of electronic communications

(1) Supervision of the use of interception and recording of telecommunications, use of surevillance of persons and items under other legislation, and interference with the operation of electronic communications is performed by the Chamber of Deputies, which for

---

[128] Act No. 273/2008 Sb. on the Police of the Czech Republic. This act is not available in English. Provided provision translated by the national rapporteur.

this purpose establishes a supervisory body. The supervisory body shall consist of MPs designated by the Chamber of Deputies.

(2) Supervision pursuant to paragraph 1 is performed by the supervisory body in the relevant police departments, after notification to the Minister. The Minister presents to the supervisory body at least twice a year a report on the use of these measures. This does not affect the right of the supervisory body to require information and participation in meetings from others.

(3) Minister shall submit to the Government, to the relevant committee of the Chamber of Deputies and to supervisory body once a year analysis of the use of measures listed in paragraph 1.

(4) The procedure in this provision is not affected by the directive on controlling.

11. Confidentiality requirements

Information about specific measures implemented to allow communication interception is classified (reserved) according to Act No. 412/2005 Sb. on the Protection of Classified Information.[129] If anyone discloses classified information to an unauthorized person, he/she may, according to Section 140 of the Act on the Protection of Classified Information, be fined for administrative offense in the amount up to 5,000,000 Czech crowns, and also prosecuted for criminal offense of endangering classified information according to Sections 317 or 318 Code of Criminal Procedure (informal translation):

Section 317 Code of Criminal Procedure – Endangering classified information

(1) Whoever pries information classified under another legal regulation with the aim to disclose it to an unauthorised person, whoever with such an aim collects data containing classified information, or whoever discloses such classified information intentionally to any unauthorised person, shall be punished by a prison sentence of up to three years or punishment by disqualification.

(2) An offender shall be punished by a prison sentence of two to eight years, if

a) they intentionally disclosed classified information to any unauthorised person under another legal regulation classed as "Top Secret" or "Secret",

b) they committed an act referred to in Subsection 1, though the obligation to protect the classified information was specifically imposed upon them, or

c) they procured a substantial benefit for themselves or another person, or they caused substantial damage or a particularly serious consequence by committing such act.

(3) An offender shall be punished by a prison sentence of five to twelve years, if

a) the act referred to in Subsection 1 relates to classified information from the area of security of the defensibility of the Czech Republic classed in another legal regulation as "Top Secret", or

b) they committed such act during a state of national emergency or war.

(4) Premeditation is punishable.

---

[129] Act No. 412/2005 Sb. on the protection of classified information. This act is not available in English.

Section 318 Code on Criminal Procedure – Endangering classified information out of negligence

Whoever, out of negligence, causes the disclosure of classified information under another legal regulation classed as "Top Secret" or "Secret" shall be punished by a prison sentence of up to three years or punishment by disqualification.

According to Section 97 para. 8 Act on Electronic Communications, ISPs and their employees are also required to maintain the confidentiality as regards any tapping or recording of messages requested or implemented and data requested or provided. The ISP may be fined up to 20.000.000 Czech crowns for violating this duty of confidentiality (Section 118 Act on Electronic Communications).

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

a) Collection of traffic data

aa) Relevant provision

The relevant provision is Section 88a Code of Criminal Procedure. It reads as follows (informal translation):

Section 88a Code of Criminal Procedure

(1) If, for the purposes of criminal proceedings conducted for an intentional criminal offence for which the law sets out a prison sentence with an upper penalty limit of at least three years, for the criminal offence of violating the confidentiality of messages (Section 182 of the Penal Code), for the criminal offence of fraud (Section 209 of the Penal Code), for the criminal offence of unauthorised access to computer systems and information media (Section 230 of the Penal Code), for the criminal offence of procuring and possessing access devices and computer system passwords and other such data (Section 231 of the Penal Code), for the criminal offence of dangerous threats (Section 353 of the Penal Code), for the criminal offence of dangerous persecution (Section 354 of the Penal Code), for the criminal offence of spreading alarming news (Section 357 of the Penal Code), for the criminal offence of encouraging a criminal offence (Section 364 of the Penal Code), for the criminal offence of approving a criminal offence (Section 365 of the Penal Code) or for an intentional criminal offence for which prosecution is stipulated in a proclaimed international treaty binding on the Czech Republic, it is necessary to ascertain data on the telecommunications service that are the subject of a telecommunications secret or that are subject to the protection of personal and intermediation data, and there is no other way to achieve the pursued purpose or if its achievement would be otherwise significantly harder, their release to the public prosecutor or to the police authority shall be ordered by the presiding judge in proceedings before the court and by the judge upon the petition of the public prosecutor in a preliminary hearing. If there are criminal proceedings for a criminal offence the prosecution of which is stipulated in such international treaty, the order for ascertaining data on the telecommunications service must be issued in writing and must be justified, including a specific reference to the proclaimed international treaty. If the request applies to a particular user, their identity must be stated in the order, if known.

(2) The public prosecutor or the police authority by whose decision the matter was finally concluded, and in proceedings before the court the presiding judge of the court of first instance after the final conclusion of the matter, shall inform the user referred to in Subsection 1, if known, of the ordered ascertainment of data on the telecommunications service. The information shall identify the court which issued the order for the ascertainment of data on the telecommunications service, and detail the period to which such order applied. Such information shall include instructions on the right to submit to the Supreme Court, within six months of receipt of this information, a petition to review the legality of the order for the ascertainment of data on the telecommunications service. The presiding judge of the court of first instance shall submit the information without undue delay after the final conclusion of the matter, the public prosecutor by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the Attorney General under Section 174a, and the police authority by whose decision the matter was finally concluded shall submit the information without undue delay after expiration of the period for the review of their decision by the public prosecutor under Section 174 Subsection 2 Paragraph e).

(3) The presiding judge, the public prosecutor or the police authority shall not submit the information under Subsection 2 in proceedings on a crime committed by an organised group for which the law stipulates a prison sentence with an upper penalty limit of at least eight years, in proceedings on a criminal offence committed for the benefit of an organised criminal group, in proceedings on the criminal offence of participation in an organised criminal group (Section 361 of the Penal Code), or if the commission of the criminal offence involved several persons and in relation to at least one of them criminal proceedings have not yet been finally concluded or if criminal proceedings are conducted against the person to whom the information is to be submitted, or if providing such information could defeat the purpose of the particular or some other criminal proceedings, or if it could threaten national security, life, health, or the rights or freedoms of individuals.

(4) An order under Subsection 1 is not required if the user of the telecommunications equipment to whom the data on the performed telecommunications service relates gives their approval for the provision of the information.

Additionally, traffic data which is not subject of a telecommunication secret or that are subject to the protection of personal and intermediation data may be requested following the procedure stipulated in Section 66 para. 3 of Act No. 273/2008 Sb. on the Police of the Czech Republic (informal translation[130]):

Section 66 Police Act – Requesting information from records

[…]

(3) The police may, in cases prescribed by the law and to extent necessary to fulfill a specific task, request from the provider of public communications network or publicly available electronic communications service traffic and location data in a manner enabling remote and continous access, unless other legal provision doesn't states otherwise. These providers are obliged to grant the access without undue delay, and in form and extent determined by other legislation.

---

[130] Act No. 273/2008 Sb. on the Police of the Czech Republic. The act is not available in English to date. Cited provision translated by national rapporteur.

bb) Substantive prerequisites of collection

Section 88a Code of Criminal Procedure specifies the types of crime for which the retained traffic data could be requested. A general requirement is that the crime being prosecuted should be intentional, i.e., one for which the law provides for imprisonment with a maximum penalty of at least three years. This, however, does not apply to the exhaustive list of crimes, which cannot be prosecuted in practice without traffic and location data, i.e., crimes committed by means of electronic communication.[131] As the Explanatory Memorandum[132] explains: "should the police during investigation of these crimes have had no chance to get traffic and location data, one could consider the decriminalization of such conduct, as these crime would be virtually inexplicable." Ultimately, the data could be also requested for the purpose of criminal proceedings against an intentional crime, which the Czech Republic is required to prosecute pursuant to an international treaty and which is binding for the Czech Republic.

The provision cited above also states that the order for the ascertainment of data on the telecommunication service can be issued only if there is no other way to achieve the pursued purpose or if its achievement would be otherwise significantly more difficult.

cc) Formal prerequisites of collection

The Public Prosecutor prepares the application for a court order to request traffic data in preliminary proceedings, usually on the basis of a written and reasoned proposal from the police authority. Before he submits the application, he must assess whether the order is necessary in order to obtain facts relevant to the criminal proceedings, whether there is no other way to achieve the pursued purpose, whether the criminal proceedings are being conducted for an adequate criminal offense, and whether he has enough information about the case to properly determine which data are to be obtained. He should mention these facts in the application, in which he also indicates the scope of the required data and formulates a proper justification.[133] The completed application is then forwarded to the judge, who evaluates

---

131 The full list with the relevant sections of Penal Code No. 40/2009 Sb. includes the following crimes: violating the secrecy of conveyed messages (Sec. 182), fraud (Sec. 209) unlawfully gained access to a computer system or data carrier (Sec. 230), acquisition and receipt of access equipment or codes for computer systems or other similar data (Sec. 231), criminal threat (Sec. 353), stalking (Sec. 354), spreading of false news (Sec. 357), incitement (Sec. 364), and criminal connivance (Sec. 365).

132 Explanatory Memorandum to Act No. 127/2005 Sb. on electronic communications and on amendment to some related laws (Act on Electronic Communications), as amended, and certain other laws. Available online in Czech: http://www.psp.cz/sqw/text/orig2.sqw?idd=84557.

133 According to the General Instruction of the Supreme Public Prosecutor No. 8/2009, on criminal proceedings.

the information provided and, if satisfied, issues the order to request traffic data. The order usually contains basically the same information as the application. The order is then forwarded to the Public Prosecutor.

dd) Duty of addressees to disclose information

The duty of addressees to retain and subsequently disclose traffic data is specifically mentioned in Section 97 para. 3 Act on Electronic Communications, which states (informal translation):

Section 97 Act on Electronic Communications – Tapping and recording messages

[…]

(3) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service shall for a period of 6 months traffic and location data which are created or processed during the operation of their public communications networks and during the provision of their publicly available electronic communications services[37b]). A legal entity or a natural person providing a public communications network or a publicly available electronic communications service is only required to store data relating to unsuccessful call attempts only when these data are created or processed and at the same time stored or recorded. At the same time, such a legal entity or natural person is required to ensure that, during the performance of the obligation referred to in the first and second sentences, no message content has been stored, and that no content thus stored has been further distributed. A legal entity or a natural person who stores traffic and location data is required, on request, immediately to provide them to:

criminal law enforcement authorities for the purposes of and under the conditions laid down in a special legal regulation[59]),

the Police of the Czech Republic for the purposes of initiating a search for a specific wanted or missing person, for the identification of persons of unknown identity or the identity of a corpse that has been discovered, for the prevention or detection of specific terrorist threats or for the verification of a protected person, while complying with the conditions set out in a special legal regulation[60]),

the Security Information Service, for the purposes of and under the conditions laid down in a special legal regulation[37]),

the Military Intelligence service for the purposes of and under the conditions laid down in a special legal regulation[37a]),

the Czech National Bank for the purposes of and under the conditions laid down in a special legal regulation[61]).

After expiry of the period referred to in the first sentence above, the legal entity or natural person who stores the traffic and location data is required to destroy them, unless they were provided to the bodies authorised to use them under a special legal regulation, or unless otherwise provided in this Act (Section 90).

(4) The traffic and location data pursuant to Subsection 3 above are primarily data leading to the tracing and identification of the source and address of the communication, and also data leading to the identification of the date, time, method and duration of the communication. The scope of the traffic and location data stored in accordance with Subsection 3 above, the form and method of their transmission to the bodies authorised to use them under a special legal regulation, and the method of their disposal is stipulated in an implementing legal regulation.

According to this provision, ISPs (of services at the IP-transport level) are required to retain specific traffic data for a period of six months. General categories of data that are subject to data retention are mentioned in para. 4 of the respective provision; a more detailed list of these data is specified in Section 3 of Decree No. 357/2012 Sb. on storing, handing over and liquidation of traffic and location data, which is not available in English. The data to be retained can be divided into two general groups:

– data used to identify the source and recipient of the data communication (telephone numbers, IMEIs, IP addresses, MAC addresses, port number, IMSI identifier, account identifier – e-mail, username, etc.);
– data used to identify the date, time, manner, and duration of a communication (communication protocol details, type of communication, time and date of communication, duration, length, etc.).

Providers of information society services (IP-application level) are not specifically required to retain any traffic data; however, they can do so with the consent of users. The extent of the data that are retained in this way varies, depending on the type of service.[134]

In practice, orders to request traffic data are usually carefully evaluated by ISPs themselves. If the order is not specific enough or does not contain all the information required by the law, they usually refuse to release the data.

ee) Automated procedure of disclosure

As far as the national rapporteur knows, as of now it is not possible to access traffic data by way of an automated online procedure. The only authority that could request traffic data from ISPs is the Unit for Special Activities. They usually send the request to the ISP via e-mail, which, after receiving the request, releases the requested data in a prescribed format. The Unit for Special Activities then forwards the data to the police authority.

b) Collection of subscriber data

aa) Relevant provision

Subscriber data can be requested from providers of a public communications network or a publicly available electronic communications service (IP-transport level services) following the same procedure as in the case of traffic data – Section 88a Code of Criminal Procedure.

---

[134] For example, social media services usually retain a lot of traffic and location data, whereas hosting providers retain just a few.

A different procedure applies if subscriber data is reqested from ISPs providing services on the IP-application level according to the Act on Information Society Services. In this case, the data may be requested according to Section 8 Code of Criminal Procedure (informal translation):

Section 8 Code of Criminal Procedure

(1) Public authorities, legal entities and natural persons are required to comply with letters of request from law enforcement authorities for the performance of their actions without undue delay and unless a special regulation stipulates otherwise, to comply without payment. Furthermore, public authorities are also obliged to immediately notify the public prosecutor or the police authorities of facts indicating that a criminal offence has been committed.

[…]

(5) Unless a special Act stipulates the conditions under which information may be disclosed for the purpose of criminal proceedings that are deemed classified pursuant to such Act or which is subject to an obligation of secrecy, such information may be requested for criminal proceedings upon the prior consent of the judge. This does not affect the obligation of confidentiality of an attorney under the Advocacy Act.

(6) The provisions of Subsection 1 and 5 shall not affect the obligation of confidentiality imposed on the basis of a declared international treaty to which the Czech Republic is bound.

bb) Prerequisites of data collection

The subscriber data may be requested from the provider of IP-application level services by means of a production order issued by the police or Public Prosecutor according to the above-cited Section 8 Code of Criminal Procedure. If the respective subscriber data are subject to an obligation of secrecy, then they can only be requested for criminal proceedings upon the prior consent of the judge (Section 8 para. 5). This, of course, does not affect the obligation of confidentiality an attorney has under the Advocacy Act.

The communication data from ISPs of IP-transport level services may be requested in cases specifically stipulated[135] in Section 88a Code of Criminal Procedure upon an order issued by a judge upon application by the Public Prosecutor. The formal requirements are the same as for the order to release traffic data.

cc) Duty of addressees to disclose information in manual and automated procedures

As far as the national rapporteur is aware, it is not possible to access traffic data by way of an automated online procedure. If the subscriber data are requested from providers of IP-transport level services (under the Act on Electronic Communica-

---

[135] If the criminal procedure is conducted for listed crimes and if there is no other way to achieve the pursued purpose or if its achievement would be otherwise significantly more difficult.

tions) according to Section 88a Code of Criminal Procedure, then the manual procedure is the same as in the case of the order to release traffic data. Here, the duty to disclose information comes from the provision stipulated in Section 97 para. 3 Act on Electronic Communications.

However, if the data are requested from providers of IP-application level services (under the Act on Information Society Services), then the police authority can request the data directly from the provider (the Unit for Special Activities is not involved). And, only if the data are subject to an obligation of secrecy, may such information be requested for criminal proceedings – only upon the prior consent of a judge. The duty to disclose the data comes from the general duty to comply with letters of request from law enforcement authorities stipulated in the above-cited Section 8 para. 1 Code of Criminal Procedure.

c) "Data retention"

The "full-scale" data retention regime was first introduced on 1 May 2005 by the Act on Electronic Communications. The act contained quite a vague formulation, which linked substantially to the implementing Decree No. 485/2005 Sb. on the extent of traffic and location data, the period of time for which such data are retained, and the manner in which they are submitted to bodies authorized to use the data that laid out the technical details. This entire data retention regulation was rather unclear and loose.

After the adoption of the directive in 2006, the act was amended by Act No. 247/2008; however, as regards the extent of the data to be retained, the Czech implementation went far beyond what was requested by the directive: the amount of transferred data, IMEI and SIM card relationships, and the type of encryption of the communication had to be retained.

After harsh criticism of the data retention regime, a group of 51 MPs and senators submitted a petition to the Constitutional Court requesting review of the constitutionality of the regime and annulment of its relevant provisions The Constitutional Court ruled on this matter in Decision No. Pl. ÚS 24/10,[136] described above in II.B.

The new version of data retention was introduced in 2012 by Act No. 273/2012 Sb., amending Act No. 127/2005 Sb. on electronic communications and on amendment to some related laws (Act on Electronic Communications) and certain other laws. The technical details were prescribed by Decree No. 357/2012 on storing, handing over and liquidation of traffic and location data. The new wording of

---

[136] Decision No. PL. ÚS 24/10. English translation available at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=c574142df486769e0b435954fead08c3

Section 97 entails a taxative enumeration of the subjects empowered to request the data. Also, the new Section 88a Act on Electronic Communications was added, which requires ISPs to ensure the security and confidentiality of the retained data as well as their destruction in an irreversible manner. According to the new wording of Section 97 Act on Electronic Communications, ISPs are required to retain specific traffic data for a period of six months.[137]

The following categories of data are subject to the data retention:

– data used to identify the source and recipient of the data communication (telephone numbers, IMEIs, IP addresses, MAC addresses, port numbers, IMSI identifiers, account identifiers – e-mails, usernames, etc.);
– data used to identify the date, time, manner, and duration of a communication (communications protocol details, type of communication, time and date of the communication, duration, length, etc.).

Section 97 Act on Electronic Communications – Tapping and recording messages

[…]

(1) A legal entity or a natural person providing a public communications network or a publicly available electronic communications service shall for a period of 6 months traffic and location data which are created or processed during the operation of their public communications networks and during the provision of their publicly available electronic communications services[37b]). A legal entity or a natural person providing a public communications network or a publicly available electronic communications service is only required to store data relating to unsuccessful call attempts only when these data are created or processed and at the same time stored or recorded. At the same time, such a legal entity or natural person is required to ensure that, during the performance of the obligation referred to in the first and second sentences, no message content has been stored, and that no content thus stored has been further distributed. A legal entity or a natural person who stores traffic and location data is required, on request, immediately to provide them to:

a) criminal law enforcement authorities for the purposes of and under the conditions laid down in a special legal regulation[59]),
b) the Police of the Czech Republic for the purposes of initiating a search for a specific wanted or missing person, for the identification of persons of unknown identity or the identity of a corpse that has been discovered, for the prevention or detection of specific terrorist threats or for the verification of a protected person, while complying with the conditions set out in a special legal regulation[60]),
c) the Security Information Service, for the purposes of and under the conditions laid down in a special legal regulation[37]),
d) the Military Intelligence service for the purposes of and under the conditions laid down in a special legal regulation[37a]),
e) the Czech National Bank for the purposes of and under the conditions laid down in a special legal regulation[61]).

---

[137] For a comprehensive overview of the legislative development around data retention, see Myška, M. Právní aspekty uchovávání provozních a lokalizačních údajů. Brno: Masarykova univerzita, 2013.

> After expiry of the period referred to in the first sentence above, the legal entity or natural person who stores the traffic and location data is required to destroy them, unless they were provided to the bodies authorised to use them under a special legal regulation, or unless otherwise provided in this Act (Section 90).
>
> (2) The traffic and location data pursuant to Subsection 3 above are primarily data leading to the tracing and identification of the source and address of the communication, and also data leading to the identification of the date, time, method and duration of the communication. The scope of the traffic and location data stored in accordance with Subsection 3 above, the form and method of their transmission to the bodies authorised to use them under a special legal regulation, and the method of their disposal is stipulated in an implementing legal regulation.

The above data retention provisions undertake another constitutional scrutiny. The Constitutional Court is expected to render its decision on constitutional compliance of the second implementation of the data retention obligations by the end of 2018.

In any case, shall specific data retention provisions be again repealed, it does not mean that traffic or location data would become inaccessible by law enforcement. Providers of electronic communication services retain respective traffic data either upon consent of users or upon specific causes such as security of their own networks. When retained for any of the above causes, traffic data will remain accessible to the law enforcement through procedural instruments that are used for discovery of stored communications – namely surrender of assets under Section 78 Code of Criminal Procedure and surveillance under Section 158d Code of Criminal Procedure.

2. Identification of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

In the Czech Republic, the identification and location of devices is easy, because such information is retained by the internet service providers ("ISPs") according to the above-cited Section 97 Act on Electronic Communications and Decree No. 357/2012 Sb. on storing, handing over and liquidation of traffic and location data. These data could also be requested from the ISP following the standard procedure described in Section 88a Code of Criminal Procedure or in Section 66 Act on the Police of the Czech Republic, which are also cited above.

Therefore, the police is not forced to use any special measures to identify or locate devices like silent SMS or IMEI-IMSI catchers.

D. Access to (Temporarily) Stored Communication Data

There is no specific provision that would allow law enforcement authorities to access stored communication data, which is why they follow procedures defined in more general provisions. The fact that regional police units work rather inde-

pendently has, in the past, led to the situation that different regions were following different general provisions for accessing communication data. For example, in the South Moravian region, the law enforcement authorities accessed remotely stored e-mails using an order to request traffic data according to Section 88a Code of Criminal Procedure, whereas, in the Pilsen region, the same data were accessed following provision Section 158d para. 3 Code of Criminal Procedure on surveillance of persons and items.

Since this situation led to many problems, the Supreme Public Prosecutor's Office decided to harmonize procedures applied by law enforcement authorities in different regions of the Czech Republic. Opinion No. 1/2015 of the Supreme Public Prosecutor's Office on harmonization of the interpretation of laws dealing with access to mobile devices and other storage media, including the content of e-mail inboxes, states that, in order to access the stored communication data, the procedure mentioned in Section 158d Code of Criminal Procedure, the surveillance of persons and items, shall be followed.

A further description of the differences between access to the data in traffic and stored data is provided above in III.B.2.a.

Section 158d Code of Criminal Procedure – Surveillance of persons and items

(1) The surveillance of persons and items (hereinafter referred to as "surveillance") means acquiring knowledge about persons and items performed in a classified manner by technical or other means. If the police authority finds during the surveillance that the accused communicates with their defence counsel, they are required to immediately destroy the records with the content of the communication, and the information that they learned in this context they are not allowed to use in any way.

(2) Surveillance during which audio, video or other records are to be obtained may be performed only upon the written authorisation of the public prosecutor.

(3) If the surveillance is to interfere with in the inviolability of residence, the confidentiality of correspondence, or finding the contents of other documents and records kept in private with the use of technology, then it may be performed only with the prior authorisation of a judge. When entering a residence, no actions other than those that lead to the planting of technical equipment can be performed.

(4) The authorisation referred to in Subsection 2 and 3 can only be issued upon written request. The request must be justified by a suspicion of specific criminal activity and, if known, with the information about the persons or items that are to be surveilled. The authorisation must state the period during which the surveillance will be carried out and this must not be longer than six months. This period may be extended by those who authorised it on the basis of a new written request, but still not exceeding six months.

(5) If the matter cannot be delayed and it is not a case referred to in Subsection 3, the surveillance may be initiated even without prior authorisation. However, the police authority is obliged to additionally request the authorisation without undue delay and if it is not received within 48 hours they are required to cease the surveillance, destroy any records, and not to use any information found in this context.

(6) Without compliance with the conditions referred to in Subsection 2 and 3, the surveillance may performed only if the person whose rights and freedoms are to be interfered with by surveillance gives their express consent. If such consent is subsequently withdrawn, surveillance shall immediately terminate.

(7) If the record of the surveillance is to be used as evidence, it is required that the transcript is attached with the particulars referred to in Section 55 and 55a.

(8) If no facts important to the criminal proceedings were found, it is necessary to destroy the records in the prescribed manner.

(9) Operators of telecommunications activity, their employees, and other persons who participate in the operation of telecommunications activity, as well as the post office or the person performing the transport of the consignments are obligated to provide the police authority performing the surveillance with the necessary assistance free of charge and in accordance with their instructions. At the same time, they may not claim the obligation of professional confidentiality imposed by special Acts.

(10) In a criminal matter other than that which the surveillance was performed for under the conditions referred to in Subsection 2, the records obtained through surveillance and the attached transcript may be used as evidence only if there is, in this case, a pending criminal proceeding on an intentional criminal offence or if the person whose rights and freedoms the surveillance interfered with, gives their consent.

1. Online searches with the help of remote forensic software

Online searches are not regulated by any specific provision. Also, there is not much experience with use of specialized remote forensic tools. However, the police probably use them even for online searches, as an investigative measure. Various forensic tools could probably be used for online searches during the general surveillance of persons and items according to Section 158d Code of Criminal Procedure. If the use of these technologies interferes with the inviolability of residence, the confidentiality of correspondence, or protection of the contents of other documents and records kept in private with the use of technology, then the search may be performed only with prior authorisation of a judge. However, because there is a lack of relevant case law, it is impossible to predict whether the use of such measures would be considered proportionate. In the opinion of the national rapporteur, use of these measures would at least interfere with the principle of proportionality and the principle of moderation formulated in the above-cited Section 2 para. 4 Code of Criminal Procedure. Evidence obtained this way would also be probably considered inadmissible, the reason being that rules on surveillance of persons and items do not provide enough safeguards. Therefore, the introduction of a specific provision will be probably necessary in the future.

There are also known cases in which such a measure was conducted by the victim in a state of self defence or extreme emergency according to Sections 28 and 29 Penal Code (informal translation[138]):

Section 28 Penal Code – Extreme emergency

(1) An act, which is otherwise criminal, whereby a person tries to avert a risk imminently threatening an interest protected by criminal law, is not a criminal offence.

---

[138] Act No. 40/2009 Sb., Penal Code. Translation taken from the legal information system ASPI.

(2) Extreme emergency shall not apply if such risk could be otherwise averted under the given circumstances, or if the consequences caused are evidently equally serious or even more serious than those imminent, or if the person at risk was obliged to endure them.

Section 29 Penal Code – Self defence

(1) An act, which is otherwise criminal, whereby a person tries to avert an imminently threatening or continuous assault on an interest protected by criminal law, is not a criminal offence.

(2) Self defence shall not apply if the defence was clearly disproportionate to the method of the assault.

Evidence gathered during use of these measures was then provided to the police authority for the purpose of criminal proceedings. There is an ongoing discussion in the Czech Republic as to whether this is legal and proportionate and whether such evidence would be admissible.

2. Search and seizure of stored communication data

a) Special provisions

There are no special provisions dealing with seizure of stored communication data in Czech criminal procedure.

b) Applicability of seizure provisions to electronic data

Police authority could seize a device or storage media in which the data has been stored (hard drives, flash drives, mobile phones, computers, etc.), following provisions on the seizure of assets (Section 79 Code of Criminal Procedure) or during house or personal searches (Section 82 Code of Criminal Procedure) (informal translation[139]):

Section 79 Code of Criminal Procedure – Seizure of assets

(1) If the asset important to the criminal proceedings is not released when those who have it in their possession are prompted, it may be removed from their possession on the warrant of the presiding judge, and in preliminary hearing, the public prosecutor or police authority. The police authority needs to have the prior approval of the public prosecutor for the issue of such warrant.

(2) If the authority that issued the warrant for the seizure of the asset does not seize such asset themselves, the police authority shall do so on the basis of the warrant.

(3) Without the prior consent referred to in Subsection 1 the warrant may be issued by the police authority only if prior approval cannot be achieved and the matter cannot be delayed.

(4) A person who is not involved in the matter shall take part in seizing the asset.

---

[139] Act No. 141/1961 Sb., Code of Criminal Procedure. Translations taken from the legal information system ASPI.

(5) The transcript of the release and seizure of the asset must also contain a sufficiently accurate description of the released or seized asset that would make it possible to determine its identity.

(6) The authority that performed the action shall immediately issue a written confirmation of the receipt of the asset, or a copy of the transcript to the person who released the asset, or from whom it was removed.

§ 82 Code of Criminal Procedure – Reasons for house and personal searches and search of other premises and land

(1) A house search can be conducted if there is a reasonable suspicion that a person or an asset important for criminal proceedings is present in the residence or other premises used for housing or on premises associated with them (residence).

(2) Due to the grounds provided for in Subsection 1 a search of non-residential premises (other premises) and land, if not publicly accessible, may be performed.

(3) Personal searches may be performed if there is a reasonable suspicion that someone is carrying an asset important to criminal proceedings.

(4) A detained person and a person who was arrested or taken into custody may even be inspected if there is a suspicion that they are in possession of a weapon or other asset that could endanger their own or someone else's life or health.

Such data can be accessed and used without further consent from the judge or Public Prosecutor.

There is also a debate as to which data are considered to be stored in the seized computer system. For example, according to some interpretations, even communication data stored in connected cloud storage may be accessed from the seized device without further consent of the judge or Public Prosecutor, because it is considered part of a computer system. There is, however, no official opinion or case law that could clarify this matter.

In addition, it remains questionable to which extent the above provisions are applicable to mere data, i.e., to simple seizure of data without seizing respective storage device or media. In practice, Section 78 (voluntary presentation of assets) is used for cases when data are requested from data subjects or ISPs and given voluntarily. For cases when voluntary discovery of data is not possible, investigators use court-approved surveillance orders pursuant to Section 158d Code of Criminal Procedure (see below).

c) Different standards of protection for stored and for transmitted data

Safeguards and requirements for the interception of communication differ from interception and access to stored data.

The interception of communication may, according to Section 88 Code of Criminal Procedure, be carried out only if respective criminal proceedings are conducted for specific crimes, if it may be reasonably assumed that facts relevant to the criminal proceedings will be obtained, and if there is no other way to achieve such pur-

pose or if its achievement would be otherwise significantly diminished. In the case of access to the stored data during surveillance of persons and items (Section 158d Code of Criminal Procedure), however, there are no such conditions.

Additionally, if the police authority wished to conduct an interception, it always requires an order issued by a judge; in the case of access to the stored data, the consent of the judge is necessary only if the interception interferes with in the inviolability of residence, the confidentiality of correspondence, or finding the contents of other documents and records kept in private with the use of technology.

Consequently, interception of communications (including traffic data) is covered with relatively more coherent and consistent safeguards compared to stored data. In particular, court orders are always required for interception of communications. On the contrary, stored data are being discovered and gathered through various procedural instruments that do not require court order, like seizure of assets (Section 79 Code of Criminal Procedure – see above) or presentation of assets (Section 78 Code of Criminal Procedure – see above), as well as through those that require court approval, such as surveillance orders under Section 158d Code of Criminal Procedure.

d) Open and clandestine access to stored data

Law enforcement authorities can, according to Section 158d Code of Criminal Procedure, access stored communication in a clandestine way during the surveillance of persons and items (informal translation):

> **Section 158d Code of Criminal Procedure – Surveillance of persons and items**
>
> (1) The surveillance of persons and items (hereinafter referred to as "surveillance") means acquiring knowledge about persons and items performed in a classified manner by technical or other means. […]

This instrument is used in cases when investigators need to obtain stored data and it is not possible to rely on cooperation of either the data subjet or respective ISP. Such surveillance order requires a court approval.

If it is possible to request voluntary cooperation by the data subject or respective ISP, investigators most frequently use request for presentation of assets under Section 88 Code of Criminal Procedure (such request does not require a court order). Such request, if served to an ISP without knowledge of respective data subject, may contain a notice that respective data subject (who is normally a suspect or another person under investigation) shall not be informed about the request. Requested ISP in that case transfers data to law enforcement not upon explicit *ad hoc* consent of respective data subject but upon general consent that was given earlier by the data subject typically in a user agreement for respective information society service.

Another instrument that is used in practice are requests for traffic data issued under Section 88a and applied *per analogiam* on stored data. This instrument, despite it might seem unreasonable, is used for stored data in cases when respective ISPs are willing to cooperate with investigators, but request a court order. This is typical situation with ISPs located abroad. Courts in that case issue traffic data orders that are neither aimed at traffic data nor they are enforceable, because they are served outside of respective jurisdictions. However, foreign ISPs often accept these orders and voluntarily provide for requested data, despite they are not bound by respective orders.

This paradoxical practice demonstrates practical operational problems caused by aforementioned absence of particular procedural instruments that would provide for proportionate and constitutionally compliant discovery or seizure of stored data.

3. Duties to cooperate: production and decryption orders

The criminal procedure contains neither production nor decryption orders. In case ISPs are willing to cooperate in discovery or gathering of stored data, investigators use general request for cooperation under Section 8 para. 1 Code of Criminal procedure or a request for presentation of assets under Section 88 Code of Criminal Procedure.

Theoretically, it would be possible to use seizure of assets under Section 89 Code of Criminal procedure to establish a duty of respective ISP to cooperate and seize and/or transfer requested data. However, this instrument is relatively weak as to its constitutional proportionality, because it does not require a court order. In result, its use might lead to inadmissibility of so gathered evidence.

Consequently, investigators currently use for establishing a duty to cooperate, depending on type of requested data, either surveillance orders issued upon Section 158d Code of Criminal Procedure or orders for traffic data issued upon Section 88a Code of Criminal Procedure. Both these orders require a court approval, so the procedure of their issue contains sufficient constitutional safeguards.

As noted above, neither orders under Section 158d nor those under Section 88a are completely fit for the purpose of forced establishment of cooperation of an ISP. This situation shall change with the introduction of currently (Fall 2018) proposed amendment to the Czech Code of Criminal Procedure that is referred to in *supra* III.A.

In any case, there are no planned amendments or other initiatives regarding decryption orders.

IV. Use of Electronic Communication Data in Judicial Proceedings

A. Use of Electronic Communication Data in the Law of Criminal Procedure

The Code of Criminal Procedure does not specifically regulate the regime of intercepted electronic communications data in criminal proceedings; thus it is necessary to follow general rules on the interception and recording of telecommunication under Section 88 Code of Criminal Procedure. This section does not make any difference between various forms of intercepted communication.

The basic requirement to order the recording of telecommunication for the criminal proceedings is the drawing up of a protocol on such order, which must fulfil statutory requirements under Section 88 para. 6 Code of Criminal Procedure; it has to fulfil certain formal conditions. Lack of fulfilment (particularly regarding information about the place, time, method of performing the recording, authority that issued the recording) can be overcome, even at the stage of criminal proceedings, in the same manner as any other formal defects of the protocol, e.g., hearing of the person who participated in the performance of the act as the witness. This cannot be considered an inadmissible manipulation in the recording of telecommunication.

The content of the recording is also an essential requirement of the protocol related to the recording of telecommunication. The transcript of each part of the communication in such recording is, however, not the essential requirement of the protocol; it is sufficient to provide information about each part of the communication concerning the time, telephone numbers (or other identification related to other types of exchange of information), and identification of the participants in the exchange of information. The procedure stated above was also confirmed by the High Court in Prague.[140] It is, however, quite customary and also recommended to present the intercepted material in transcribed form to the court.

Another important aspect when introducing the recording as evidence in the criminal proceedings is its unaltered form. Assuming that, in the specific case, there is no apparent devaluation or any other reduction in the information value of the evidence, the applicability of the evidence in the criminal proceedings is not affected in any way. Technical measures to compress the content of intercepted communication cannot therefore be considered as unauthorized interference with the evidence in accordance with Section 88 Code of Criminal Procedure (such as

[140] The decision of the High Court in Prague dated 18 January 2001, file number 4 To 3/01. In: beck-online [legal information system].

the compression of the communication on a data carrier). The use of only a part of the communication related to the criminal case is also considered admissible.[141]

B. Inadmissibility of Evidence as a Consequence of Inappropriate Collection

It is not permissible to exclude any type of evidence except in cases in which the Code of Criminal Procedure indicates the inadmissibility of certain means of evidence, procedure, or act.[142] The Code of Criminal Procedure, however, does not contain any further statement, which would require explicit enumeration of all the cases of inadmissible evidence. This is why it is necessary to follow general requirements on the admissibility of evidence under the Code of Criminal Procedure and with respect to the proceedings.[143] The inadmissibility of evidence is therefore deduced mainly from the interpretation of the provisions. There are two main approaches of the Constitutional Court to the inadmissibility of evidence as to whether there was any misconduct in obtaining the evidence. The first concept is based on the fact that the evidence is inadmissible because of the prohibition of arbitrari-

---

[141] This opinion was confirmed by the Supreme Court. The decision of the Supreme Court dated 24 June 2009, file number 5 Tdo 572/2009. In: beck-online [legal information system].

[142] Section 89 para. 2. Code of Criminal Procedure. In: ASPI [legal information system]:
Evidence may be anything that may help to clarify matters, in particular the testimonies of the accused and witnesses, expert opinions, items and documents relevant to the criminal proceedings, and examinations. Each party may seek, submit, or propose the implementation of evidence. The fact that the law enforcement authority did not seek or request it is not grounds for the rejection of such evidence.

Section 89 para. 3. Code of Criminal Procedure. In: ASPI [legal information system]:
Evidence obtained by unlawful coercion or threat of coercion may not be used in the proceedings except when used as evidence against the person that used coercion or threatened coercion.

[143] It is also necessary to keep Section 8c and Section 30 para. 4 Code of Criminal Procedure in mind.

Section 8c Code of Criminal Procedure. In: ASPI [legal information system]:
Pursuant to Section 88 no person shall disclose information on the court order or interception performance and recording of telecommunications traffic without the consent of persons whom such information concerns or information derived thereof, data on telecommunications traffic detected on the basis of an order under Section 88a, or information obtained by the surveillance of people and items under Section 158d Subsection 2 and 3, if such information allows the identification of the person and if such were not used as evidence in proceedings before the court.

Section 30 para. 4 Code of Criminal Procedure. In: ASPI [legal information system]:
The judge who took part in the decision making process of the earlier proceedings is excluded from the proceedings on the review of the order for the interception and recording of telecommunications traffic. The judge who participated in the decision making process on the review of the order for the interception and recording of telecommunications traffic is further excluded from the decision making process of the subsequent proceedings.

ness, which sets out the obligation of the courts and other criminal proceedings authorities not to deviate in any way from the rules of procedure.[144] The second approach is based on infringement of the right to a fair trial through a breach of right of another person, e.g., privacy rights.

Specific questions connected with the inadmissibility of the interception (Section 88 Code of Criminal Procedure) are described subsequently. Generally, the records of communication of a person that were acquired against the law (especially if the conditions under Section 88 were not fulfilled) are taken as absolutely inadmissible evidence. Transcripts of such recordings cannot be filed in the criminal file. If this happens, the transcript, as well as the records themselves, cannot be used in criminal proceedings as evidence.[145]

On the basis of Section 88 para. 1 sentence 3 Code of Criminal Procedure, the interception and recording of telecommunication between the defence counsel and the accused only is inadmissible and it has to be destroyed. Such prohibition does not apply, however, to the communication of the accused person with his/her family members.[146] It is also necessary to fully follow the conditions stipulated under Section 88 para. 6[147] to attach the protocol containing the information specified above[148] in order to be able to use the evidence in the criminal proceedings. Only the recordings of telecommunication, relevant for the case may be included in the criminal case file. Other communication in the meaning of Section 88 para. 6 must be protected against unauthorized use and kept outside the criminal case file. It is especially necessary to protect personal data and third person data contained in the records, which has no connection to the criminal proceedings.[149]

---

144 The decision of the Constitutional Court dated 3 March 2005, file number III. ÚS 501/04. In: beck-online [legal information system].

145 The decision of the Regional Court in České Budějovice dated 29 September 1994, file number 4 To 354/94. In: beck-online [legal information system].

146 The decision of the Supreme Court dated 15 June 2011, file number 4 Pzo 3/2011-37. In: beck-online [legal information system].

147 Section 88 para. 6. Code of Criminal Procedure. In: ASPI [legal information system]:
If the record of the telecommunications service is to be used as evidence, it is necessary to accompany it with the transcript, giving the place, time, manner and contents of the record, as well as the authority which issued the record. The police authority is obliged to label other records, securely store them so as to protect them against unauthorised misuse, and indicate the place of storage in the transcript. In another criminal case other than the one in which the interception and recording of telecommunications service was performed, the recording may be used as evidence if there is a criminal prosecution in this matter for a criminal offence referred to in Subsection 1, or with the consent of the user by the intercepted station.

148 The decision of the High Court in Prague dated 18 January 2001, file number 4 To 3/01. In: beck-online [legal information system].

149 The decision of the Constitutional Court dated 16 September 2010, file number III. ÚS 3221/09. In: beck-online [legal information system].

The interception and recording of telecommunication for the purpose of criminal proceedings is governed by the provisions of Section 88 Code of Criminal Procedure. This allows taking such action, also before the commencement of the prosecution, but only in the case of emergency and urgent operations. The interception can be used in criminal proceedings only if it was conducted on the basis of Section 88 Code of Criminal Procedure. Interception carried out under amy other legal act, e.g., under Act No. 283/1991 Sb. on the Police of the Czech Republic or under Act No. 13/1993 Sb., Customs Act, can be used only for the purposes defined by these acts (the means of operative techniques). This must be respected even if the evidence was collected under the same conditions that would otherwise be sufficient to carry out urgent interception according to the Code of Criminal Procedure. Records of such interception (and the interception itself) as well as any other operative technique materials cannot be used as evidence.[150] It was decided previously by the European Court of Human Rights in the case of *A. v. France* that interference with privacy with the attendance of police authorities was found to breach Art. 8 Convention for the Protection of Human Rights and Fundamental Freedoms (in this case, a detained suspected hitman, in cooperation with the police, recorded a phone call in which suspected persons revealed the details of the murder).[151]

Despite the fact that the evidence was obtained in violation of the law, such evidence may still be used in criminal proceedings. The Constitutional Court stated that in order for an audio recording recorded by a private person without the consent of the person whose voice was recorded to be used as evidence, it is necessary to consider firstly whether the evidence in the form of, e.g., an audio recording on a cell phone of the witness stands alone in a concrete situation when evaluating the guilt of the offender or whether the court also has other evidence at its disposal, which significantly supports the merits of the accusation and which is also supported by such recording of the conversation.[152] The information contained in the recording can serve as evidence in criminal proceedings only if the invasion of privacy is justified by the overriding interests of the person who provided the information in the manner described and then used. According to the opinion of the courts, illegally taken recording can be used only as supportive evidence to verify the facts stated in both interception and witness testimony.[153] Given the fact that

---

[150] The Act on the Police of the Czech Republic and the Customs Act have been amended; however, the decision of the High Court serves as an example of narrow interpretation of the possibility to use the intercepted evidence in criminal proceedings. The decision of the High Court in Prague dated 8 June 2000, file number 2 To 73/2000. In: beck-online [legal information system].

[151] *A. v. France*, decision of 23 November 1993, Application No. 14838/89. In: HUDOC [legal information system].

[152] The decision of the Constitutional Court dated 20 October 2011, file number II. ÚS 143/06. In: beck-online [legal information system].

[153] This was confirmed by the decision of the Supreme Court of 3 May 2007, file number 5 Tdo 459/2007 or by the decision of the Supreme Court of 25 September 2013, file number 8 Tdo 908/2013. In: beck-online [legal information system].

there are rules on interception of the recording of telecommunication by the authorities that allow (among other data) acquiring the content of telephone messages, it is also possible to follow these rules when acquiring these "other" data, i.e., during the process of recording the telecommunication.[154]

It is necessary to state since when the intercepted communication can be used as evidence in criminal proceedings, e.g., the example of cell phones. In criminal proceedings, cell phones are perceived as any other tangible assets. The data stored on cell phones are evaluated in a similar way. The authorities in criminal proceedings can therefore extract all the data stored on the phone and such evidence can be used in criminal proceedings. But it is necessary to distinguish the specific moment at which the communication was taking place and to distinguish the use of various procedural instruments.[155] This was confirmed by the Explanatory Opinion of the Supreme Public Prosecutor's Office No. 4/2005.[156] Following this opinion, the police authorities do not need an interception order from the judge (issued on the basis of Section 88 Code of Criminal Procedure) if the data had already been delivered and present on the cell phone even before the moment at which the police authority took the cell phone into its possession.[157] This means that all the data stored on the cell phone at the moment of securing it may be used as evidence.

In the case of uncollected voicemail, it is necessary to issue an interception order according to Section 88 Code of Criminal Procedure. Voicemail (unlike unread SMS message) is not stored directly on the mobile phone. It can only be collected from the data storage of a service provider through the cell phone. Such data cannot be used as evidence in the criminal proceedings only on the basis of seizure of assets proceedings. It was stated in the Explanatory Opinion of the Supreme Public Prosecutor's Office No. 1/2015 that it is necessary to issue an interception order prior to the commencement of the communication itself if the voicemail is planned to be used as the evidence.[158]

---

[154] The decision of the Constitutional Court dated 22 January 2001, file number II. ÚS 502/2000. In: beck-online [legal information system].

[155] Such interpretation was confirmed by the decision of the Supreme Court dated 15 December 2000, file number 7 Tz 9/2000. In: beck-online [legal information system].

[156] The Supreme Public Prosecutor's Office, SL 788/2004, The Collection of the Explanatory Opinions of the Supreme Public Prosecutor's Office, No. 4/2005, in Brno 6 June 2005, accessible at: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2005/stanovisko%204-2005.pdf. This opinion also stated that the data stored in the SIM card inserted in the cell phone have the same status as the data stored directly in the cell phone.

[157] It is necessary to state that securing of the cell phone was issued under different provisions than the provision concerning interception. In this case, the proceedings are stated in Section 78 (presentation of assets) and Section 79 (seizure of assets) Code of Criminal Procedure. In: ASPI [legal information system].

[158] The Supreme Public Prosecutor's Office, 1 SL 760/2014, The Collection of the Explanatory Opinions of the Supreme Public Prosecutor's Office, No. 1/2015, in Brno

The communication, which is not statically stored via secured remote service or storage but is still the subject of electronic communications (e-mail or other messenger communication services), has a special position. The Explanatory Opinion states that the provider of electronic communications is not entitled to store and to transfer message content.[159] The Supreme Public Prosecutor's Office then concludes on the basis of such statement that Section 88 Code of Criminal Procedure can be only used for realtime communication. The communication (in the past or in the present) provided through information society services is, however, recorded and stored. Such communication (e-mail, online messengers) could not be provided in the meaning of its general purpose without the possibility to store the information. Thus, if the communication was stored on any device, there should be no limitation to using such data (despite the facts stated by the Explanatory Opinion) after the moment the interception order is properly issued. If the device was already seized as the communication was still ongoing (e.g., unread e-mail), it will still be necessary to issue an interception order on the basis of Section 88 Code of Criminal Procedure.

If the evidence (interception) was acquired legally, it cannot be excluded by the court only because of the fact that the legal regulation on evidence proceedings has changed. The legality of such proceedings is decided on the basis of the legal regulation that was in the force at the time the measures to acquire such evidence were taken.[160]

When investigating serious crimes, the police can interfere in a lawful manner with different developmental stages of a criminal offense. It cannot provoke (initiate) the criminal activity that would not be committed without such provocation. The opinion that the duty of the police is always to prevent the commission of the criminal offense in its initial stage would prevent the use of operative and investigative methods (interception). This would make such methods useless and would lead to paralysis on the part of the police to carry out its tasks in the process of detection of serious criminal offenses and to reveal the identity of the offender. It is also necessary to address the question of culpability in relation to the application of a higher criminal sentence when deciding whether the requirement of Section 88 para. 1[161] is fulfilled or not.[162]

---

26 January 2015, accessible at: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf

[159] The Supreme Public Prosecutor's Office, 1 SL 760/2014, The Collection of the Explanatory Opinions of the Supreme Public Prosecutor's Office, No. 1/2015, in Brno 26 January 2015, accessible at: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf. p. 8.

[160] The decision of the Constitutional Court dated 7 May 2014, file number Pl. ÚS 47/13. In: beck-online [legal information system].

[161] The interception can be used only in the case of serious crimes, thus it is necessary to consider whether such crime described in Section 88 para. 1 had really been committed.

From the point of view of constitutionally protected fundamental rights, it is highly inadmissible that, for clarification and verification of the facts indicating that the crime was committed (commencement of operations), it cannot be allowed to use interception to subsequently justify that a serious crime (under Section 88 para. 1) has been committed.[163]

In its decision, the Constitutional Court strongly stressed that, if there are any specific facts supporting the suspicion for committing a serious crime, then, with regard to the constitutional limits of regulation of interception, such facts have to be clearly apparent in the rationale of the interception order. The specific rationale, however, contained only very vague argumentation to support the suspicion that a person was in attendance during a particular criminal action. The interception order did not include specific facts from which it was clear that a particular person was suspected of committing the criminal offense. It is necessary to use proper and persuasive argumentation in the interception order on why it was decided to use such a strong procedural instrument as interception.[164] Without proper rationale in the interception order, the information gained on this basis cannot be used in the criminal proceedings.

The facts stated above serve as the general concept on how the limitation and consideration of the admissibility of interception as evidence works in the criminal proceedings. It relied especially on the rulings of the higher courts. If the limits indicated above are exceeded, the use of interception as evidence cannot be found to be legitimate; thus, the communication data contained in the interception will be regarded as illegally obtained.

C. Use of Data outside the Main Proceedings

1. Data from other criminal investigations

The interception and recording of telecommunication can be used in another criminal case as evidence under the condition that:

– In such another criminal case, there is a criminal prosecution for criminal offense referred in Section 88 para. 1 Code of Criminal Procedure. These are crimes for which the law stipulates a prison sentence with the maximum limit of at least eight years (machinations in insolvency proceedings, violation of regulations on rules of competition, negotiating advantages during public procurement/tender and auction, misuse of powers of an official person or for any other intentional

---

[162] The decision of the High Court in Prague of 19 January 2006, file number 2 To 139/2005. In: beck-online [legal information system].

[163] The decision of the Constitutional Court dated 27 September 2014, file number II. ÚS 789/06. In: beck-online [legal information system].

[164] The decision of the Constitutional Court dated 27 January 2010, file number II. ÚS 2806/08. In: beck-online [legal information system].

criminal offense for which prosecution is stipulated in a declared international treaty), or

– with the consent of the user of the intercepted station (anyone who uses or requests a publicly available electronic communications service).[165]

It should be stated that, if there was an interception order issued on the basis of commission of a serious criminal offense (as stated in Section 88 para. 1 Code of Criminal Procedure), in the first case of criminal prosecution, then the fact that the criminal prosecution against the same person for another criminal offense (which was, however, not serious criminal offense mentioned in Section 88 para. 1) was initiated after that, does not mean that the interception would be illegal against that person. The interception cannot, however, be used as evidence for a second and less serious offense; it can be used to support the facts only in the first case of criminal prosecution.[166]

The requirements that have to be contained in the interception order are listed in Section 88 para. 2 Code of Criminal Procedure:

> The interception order and recording of the telecommunications service shall include a determined user address or a user device and the user if their identity is known, and the period during which the interception and recording of telecommunications traffic is conducted cannot be longer than four months; the justification must include the specific facts that justify the issue of such order as well as its period.

In the case of possible use of the intercepted data for the prosecution of individuals who were not the subject of the interception order, it has to be concluded that, if there was already ongoing interception, evidence on the basis of such interception can also be used for the criminal offense that was discovered during the interception. This evidence can, however, be used if the discovered criminal offence fulfils the conditions of serious crime listed in Section 88 para. 1. If these conditions are fulfilled, then it is not relevant whether the interception was allowed and the recording acquired regarding the suspect, accused, or any other person.[167]

2. Data from preventive investigations

The case law of the European Court of Human Rights, in limiting the fundamental right to privacy for security reasons, strictly restricts the conditions for the ap-

---

[165] Section 88 para. 6 sentence 3 Code of Criminal Procedure. In: ASPI [legal information system]. The wording of Section 88 para. 6 was enacted in 1 July 2008, but the use of evidence in other criminal offence proceedings under certain conditions had already been expressed in the decision of the Constitutional Court of 27 April 1994, file number II. ÚS 6/93. In: beck-online [legal information system].

[166] The decision of the Supreme Court dated 13 April 2011, file number 4 Pzo 2/2010. In: beck-online [legal information system].

[167] The decision of the Supreme Court dated 9 October 2003, file number 2 To 144/03. In: beck-online [legal information system].

plicability of evidence obtained by limiting privacy. It approves only such practices, which can offer adequate safeguards to protect fundamental rights, e.g., against abuse or arbitrariness because, in the opposite case (and also because of present technological possibilities), democracy itself is at stake. This principle was also highlighted in the case of *Klass and others v. Germany* (especially in paras. 42, 48, 49, 50).[168]

Based on the above-mentioned arguments, the Constitutional Court considered the possibility of using interception outside the criminal proceedings (intelligence service) in criminal proceedings. Interception of communication by public authorities (as well as any other type of secret surveillance) represents a serious limitation of fundamental rights. It is implied from the interception order that the limitation of personal integrity and privacy may very rarely be made by public authorities, only when necessary and if the aim of pursuing public interest cannot otherwise be achieved. Failure to comply with certain conditions means that such action is unconstitutional.

Intelligence law incorporates less limiting rules on the breach of privacy; these milder conditions are only tolerated when limited by strict intent of the use of the gathered information and also by the seriousness of possible danger.

Using intelligence interception in criminal proceedings as evidence of guilt is foreseen neither in the Code of Criminal Procedure nor in the law on intelligence services. In concrete cases, interceptions were acquired pursuant to the act relating to the intelligence services. The intelligence service crossed the boundaries of the law when it provided a highly concretized, extensive set of information to the authorities prosecuting a criminal offence. Intelligence services in relation to criminal proceedings law are only entitled to provide basic and general information (Section 8 para. 3 of Act No. 153/1994 Sb. on intelligence services of the Czech Republic). Any use of interception outside the sphere of application of the law on intelligence services was and is an ongoing violation of fundamental human rights. It was explicitly stated that the potential threat of terrorist attack also cannot breach the barrier of constitutional mechanisms.[169]

3. Data from foreign jurisdictions

The questions on acquiring, using, and admitting evidence of intercepted data abroad are regulated mainly by Act No. 104/2013 Sb. on international judicial cooperation in criminal matters. This law deals with issues of interception in Section 47, where the possibility to provide legal assistance to another state based on

---

[168] *Klass and others v. Germany*, decision of 6 September 1978, Application No. 5029/71. In: HUDOC [legal information system].

[169] The decision of the Constitutional Court dated 29 February 2008, file number I. ÚS 3038/07. In: beck-online [legal information system].

the principle of reciprocity is established. This section, however, states that it is unconditionally necessary to respect the rules incorporated in the Code of Criminal Procedure.

If an international treaty stipulates that the interception can be carried out by a foreign country on the territory of the Czech Republic without the technical assistance of the Czech Republic, the Regional Court in Prague is responsible for deciding on the consent to interception or its continuation; if a preliminary procedure is conducted in the foreign state, which will perform the interception, the Public Prosecutor from the Regional Prosecutor's Office in Prague decides on the admissibility of such interception. Consent to interception or its continuation can be granted only if the conditions set out in Section 88 Code of Criminal Procedure are fulfilled.[170]

If an international treaty stipulates that it is possible to carry out the interception of telecommunication from the Czech Republic on the territory of a foreign state without its technical assistance, the prosecutor and – after filing the indictment – the court informs the foreign state about the anticipated interception in the manner provided by that international treaty.[171]

The general rule to respect the requirements under Section 88 Code of Criminal Procedure has also been highlighted by the Supreme Court in the past and before Act No. 104/2013 Sb. on international judicial cooperation in criminal matters was in force. It was also stressed that it is necessary to rationalize intervention into privacy in this decision.[172]

D. Challenging the Probity of Intercepted Data

According to Section 88 para. 8 Code of Criminal Procedure, after the criminal case becomes final, the prosecutor or the presiding judge of the court of first instance informs the person who is the user of the device about the interception order and the recording of telecommunication, unless exceptions under Section 88 para. 9 are fulfilled.[173] Such person may submit a proposal to review the legality of the

---

[170] Section 64 para. 1. Act No. 104/2013 Sb. on international judicial cooperation in criminal matters. In: beck-online [legal information system].

[171] Section 64 para. 2. Act No. 104/2013 Sb. on international judicial cooperation in criminal matters. In: beck-online [legal information system].

[172] The decision of the Supreme Court dated 13 April 2007, file number 11 Tz 129/2006. In: beck-online [legal information system].

[173] Section 88 para. 9. Code of Criminal Procedure. In: ASPI [legal information system]: The presiding judge, the public prosecutor or the police authority does not submit the information under Subsection 8 in proceedings on a crime committed by an organised group for which the law stipulates a prison sentence with the upper penalty limit of at least eight years, in proceedings on criminal offences committed for the benefit of an organised criminal group, in proceedings for criminal participation in an organised criminal group (Sec-

interception to the Supreme Court within six months; the Supreme Court, in proceedings under Section 314l–314n[174] Code of Criminal Proceedings, by resolution, either rules that the law was violated or declares that the law was not violated. This decision is not subject to appeal.

The prerequisite for filing a petition before the Supreme Court for review of the legality of interception in accordance with Section 314l is Section 88 para. 8, accordingly that the case was ended. It is also necessary that the presiding judge of the court of first instance or the prosecutor subsequently inform the person authorized to file such petition about the ordered interception. A proposal to review the legality of interception cannot therefore be submitted to the Supreme Court before the relevant case is final and without subsequent sending of the information to the authorized person. If such petition is filed, even if the above stated conditions were not fulfilled, the Supreme Court rejects it as inadmissible.[175]

In accordance with Sections 314l et seq. Code of Criminal Procedure, in the procedure for review of an interception order, review by the Supreme Court is limited to only the assessment of legality of the issued interception order and the recording of telecommunication. Therefore, in these proceedings, the Supreme Court cannot

---

tion 361 of the Penal Code), or if the criminal offence involved more people and in relation to at least one of them the criminal proceedings have not yet been finally concluded or if it is against the person to whom the information was submitted, is the subject of criminal proceedings, or if providing such information could defeat the purpose of the criminal proceedings, including those referred to in Subsection 6, or if it could lead to threats to national security, life, health, or the rights and freedoms of individuals.

[174] Section 314l Code of Criminal Procedure. In: ASPI [legal information system]:
(1) Upon the petition of the person referred to in Section 88 Subsection 8, the Supreme Court, in closed hearing, shall examine the legality of the warrant for the interception and recording of the telecommunications service.

(2) Upon the petition of the person referred to in Section 88a Subsection 2, the Supreme Court, in closed hearing, shall examine the legality of the order for the ascertainment of data on the telecommunications service.

Section 314m Code of Criminal Procedure. In: ASPI [legal information system]:
(1) If the Supreme Court finds that the warrant for the interception and recording of the telecommunications service or the order for the ascertainment of data on the telecommunications service was issued or its performance was contrary to law, they shall pronounce the violation of the law by a resolution.

(2) An appeal against such decision is not permissible.

Section 314n Code of Criminal Procedure. In: ASPI [legal information system]:
(1) If the Supreme Court finds that the warrant for the interception and recording of the telecommunications service was issued and its performance was in compliance with the conditions set out in Section 88 Subsection 1 or the order for the ascertainment of data on the telecommunications service was issued and its performance was in compliance with the conditions set out in Section 88a Subsection 1, they shall pronounce in a resolution that the law was not violated.

(2) An appeal against such decision is not permissible.

[175] The decision of the Supreme Court dated 14 October 2010, file number 4 Pzo 1/2010. In: beck-online [legal information system].

deal with, e.g., any objection related to the performance of duties of the police authority in accordance with Section 88 para. 3 or objections against the evaluation of the results of the interception directed against the rationale of the court, which decided such interception.[176]

Under the conditions of Section 88 paras. 1, 2, it is also exceptionally possible to also order the interception during the phase of enforcement proceedings in connection with the search of a convicted person who is meant to be imprisoned for the offence listed in Section 88 para. 1. It is, however, permitted to use the interception only when any other procedures on how to locate such person have failed. The legality of such interception can also be examined by means of the procedure described under Sections 314l–314n.[177]

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

International conventions on MLA have priority of application in Czech Law according to the Art. 10 of Act No. 1/1993 Sb., Constitution of the Czech Republic. Specifically, for MLA this is also listed in Art. 3 para. 2 of Act No. 104/2013 Sb. on International Judicial Cooperation in Criminal Matters.

Art. 10 [informal translation]

Promulgated international agreements ratified by the Parliament and binding the Czech Republic are part of law; if the agreement differs from the Act, international agreement shall be used.

Art. 3 para. 2 [informal translation]

This Act governs the procedure, unless the international conventions stipulates otherwise.

Therefore, the application of national legislation is directly related to the absence of international agreement regulating the same topic. Application of national legislation is also possible when an international convention does not regulate the topic in sufficient detail. This is the case for both multilateral and bilateral agreements.

1. International conventions

The Czech Republic has signed and ratified the following conventions:

---

[176] The decision of the Supreme Court dated 13 April 2011, file number 4 Pzo 2/2010. In: beck-online [legal information system].

[177] The decision of the Supreme Court dated 5 June 2013, file number Tpjn 304/2012. In: beck-online [legal information system].

– European Convention on Mutual Assistance in Criminal Matters, 1959, promulgated as no. 550/1992 Sb.
– Additional Protocol to the European Convention on Information on Foreign Law, 1978, promulgated as no. 31/1997 Sb.
– Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, 2001, promulgated as no. 48/2006 Sb. m. s.
– Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 2000, promulgated as no. 55/2006 Sb. m. s.
– Additional Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 2001, promulgated as no. 56/2006 Sb. m. s.
– European Convention on Extradition, 1957, promulgated as no. 549/1997 Sb.
– Additional Protocol to the European Convention on Extradition, 1975, promulgated as no. 29/1997 Sb.
– Second Additional Protocol to the European Convention on Extradition, 1978, promulgated as no. 30/1997 Sb.
– Third Additional Protocol to the European Convention on Extradition, 2010, promulgated as no. 34/2013 Sb. m. s.
– Convention on Cybercrime, 2001, promulgated as no. 104/2013 Sb. m. s.
– United Nations Transnational Organized Crime Convention, 2000, promulgated as 75/2013 Sb.

The Czech Republic has signed and ratified many other international agreements shaping its penal policy and firmly placing it within the international framework.[178] However, the above-mentioned agreements currently have the biggest influence on MLA in the Czech Republic.

2. Bilateral treaties

The Czech Republic has signed and ratified the following bilateral treaties involving Germany:

– Agreement between the Czech Republic and the Federal Republic of Germany on amendments to the European Convention on Mutual Assistance in Criminal Matters, promulgated as no. 68/2002 Sb. m. s.
– Note of the Ministry of Foreign Affairs of the Czech Republic of June 19, 2002 on change of designation and jurisdiction of organs listed in Art. 19 para. 1 and Art. 20 para. 4 of the Agreement between the Czech Republic and the Federal

[178] Agreements on prohibition and punishment of white slave trade, trade in women of full age, genocide, etc.

Republic of Germany on amendments to the European Convention on Mutual Assistance in Criminal Matters, promulgated as no. 126/2002 Sb. m. s.

– Note of the Ministry of Foreign Affairs of the Czech Republic of September 8, 2005 on change of designation and jurisdiction of organs listed in Art. 19 para. 1 and Art. 20 para. 4 of the Agreement between the Czech Republic and the Federal Republic of Germany on amendments to the European Convention on Mutual Assistance in Criminal Matters, promulgated as no. 124/2005 Sb. m. s.
– Note of the Embassy of the Federal Republic of Germany of January 5, 2006 on change on change of designation and jurisdiction of organs listed in Art. 23 para. 3 no. 2 b) of the Agreement between the Czech Republic and the Federal Republic of Germany on amendments to the European Convention on Mutual Assistance in Criminal Matters, promulgated as no. 30/2006 Sb. m. s.

The first above-mentioned bilateral agreement stipulates in Art. 17 special methods of investigation and cooperation, which are relevant for the purpose of electronic communication interception. The incoming request can be taken further only if it is submitted by the court or accompanied by the statement of the court from which it is clear that all the conditions for interception would be met if the interception were to take place within the territory of the state issuing the request. The purpose of this provision is to ensure that the issuing state is not able to deliberately lower the standard of procedural checks. The second condition that has to be met is that the interception warrant could be issued by the state receiving the request. The purpose of this provision is to ensure that the receiving state does not warrant interception that would have otherwise been unlawful. Also, the interception can proceed further only if the person or device subjected to interception is located within the territory of the state receiving the request; or located within the state issuing the request but the interception cannot be carried out without the cooperation of the state receiving the request; or within the territory of the third state but the state issuing the request needs the technical assistance of the state receiving the request.

The second, third, and fourth of the above-mentioned bilateral agreements reflected organizational changes within both Czech and German law enforcement. Therefore, they did not bring about any substantial change to the matter of electronic communication interception itself.

It is also possible to seek legal assistance without multilateral or bilateral agreements. In this case, the Ministry of Justice needs to issue a confirmation of reciprocity.[179] This is even preferable, according to some experts, because the absence of international conventions allows them to follow less formal procedures.[180]

---

[179] In case the confirmation has already been issued, notice can be found on the Intranet of prosecutors.

[180] Comp. Novotná, J.: Právní pomoc v cizím státu v přípravném řízení trestním. 3. vydání. Praha : C.H. Beck, 2015, p. 212.

3. National regulation

Act No. 104/2013 Sb. on Mutual Judicial Assistance in Criminal Matters [Zákon o vzájemné justiční spolupráci ve věcech trestních] (hereinafter referred to as ZMJS) is the main legal instrument governing judicial MLA at the national level.

ZMJS was adopted only recently and has been in effect since the 1 January 2014.[181] However, this creates only mild interpretational problems, since most of the provisions were previously contained in Act No. 141/1961 Code of Criminal Procedure [Trestní řád]. Nonetheless, warranting an interception in the case of MLA is extremely rare (see statistics below). Usually, MLA does not seek to obtain the warrant but merely seeks to receive the evidence already obtained for the purpose of criminal proceedings abroad.

Overall, for the purpose of electronic communication interception in another state, the law does not foresee any special procedure. Standard requests in accordance with international conventions, possible bilateral treaties, or general provisions of ZMJS can be submitted.

However, the special case of cross-border interception is contained in the law and is governed by Art. 64 of ZMJS. The Czech national regulation requires explicit permission by multilateral or bilateral agreement in order to use cross-border interception without the technical assistance of the other state.

B. Requirements and Procedure (Including the Handling of Privileged Information)

1. Incoming requests

The procedure is fairly straightforward and follows the conditions set out in Art. 18 para. 3 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

> **Art. 18 para. 3 Convention on Mutual Assistance in Criminal Matters** [official translation]
>
> By way of derogation from Article 14 of the European Mutual Assistance Convention and Article 37 of the Benelux Treaty, requests under this Article shall include the following:
>
> (a) an indication of the authority making the request;
>
> (b) confirmation that a lawful interception order or warrant has been issued in connection with a criminal investigation;
>
> (c) information for the purpose of identifying the subject of this interception;
>
> (d) an indication of the criminal conduct under investigation;

---

[181] Previous national regulation was contained in Act No. 141/1961 on criminal procedure [Trestní řád].

(e) the desired duration of the interception; and
(f) if possible, the provision of sufficient technical data, in particular the relevant network connection number, to ensure that the request can be met.

However, certain problem might appear concerning the admissibility of the evidence obtained in this way. According to Art. 42 para. 2 ZMJS, the interception can be used for the purpose of Czech criminal procedure if it was obtained in accordance with either foreign or Czech provisions. The Supreme Court ruled on this in its Decision on Case 11 Tz 129/2006 of 13 April 2007, in which it was concluded that, once the requirements prescribed by Czech law are met, nothing prevents the evidence obtained by interception of communication from being used in Czech criminal procedure, even if obtained abroad.

Two organs handle the incoming requests. At the pre-trial stage, the responsible organ is the Department of International Affairs of the Supreme Public Prosecutor's Office. The responsible organ at the trial stage is the International Department for Criminal Matters of the Ministry of Justice of the Czech Republic. The request is then passed to the organ responsible for issuing a warrant for the purpose of pre-trial or trial proceedings. The national law does not prescribe any special procedure, save for the above-mentioned responsible organs. There is no duty to filter or delete the privileged information from the intercepted communication.

Art. 42 para. 2 Convention on Mutual Assistance in Criminal Matters [informal translation]

Evidence obtained at the request of the judicial authority of the foreign authority may be used in criminal proceedings in the Czech Republic only if they were acquired in accordance with the laws of the foreign country, or in accordance with Czech law.

2. Outgoing requests

Any procedures needed to intercept electronic communications are followed in the foreign state and by its organs; therefore, the Czech Republic and its organs do not have to issue a warrant. The foreign body is generally satisfied with the content of the request for legal assistance provided by the Public Prosecutor – the prosecutor, however, must assure the foreign organ that all the conditions laid down by Czech law have been met. Then, the foreign organ issues the warrant normally prescribed by its own national law. However, if the foreign organ refuses to issue its own warrant with the argument that it cannot be done without a Czech warrant, the prosecutor requests the warrant and it is then transferred to the foreign organ according to Art. 45 ZMJS.

The special situation of cross-border interception that was already mentioned above is not, *stricto sensu* a request for a warrant. It serves mainly to inform the foreign state that the Czech Republic will be performing the interception itself within the foreign jurisdiction without the need for technical assistance. Therefore, the principle *locus regit actum* is violated, because Czech law governs the intercep-

tion. Also, the criminal jurisdiction of the foreign state is violated, because the Czech organs will perform the interception. This is the main reason why this is possible only if permitted *expressis verbis* by the international agreement.

3. Technical regulation

The technical regulation of every interception of communication data involves the following measures:

- file material exists in four places – ÚZČ (Útvar zvláštních činností, "the Unit for Special Activities of Criminal Police and Investigation", specialized department within the Czech police responsible for deployment of interception of communication), authorized body (department requesting the interception of communication), Public Prosecutor, and the court;
- request can be edited only by the department possessing the files for the specific interception;
- system can be accessed only by the authorized person, based on individual authentication information;
- log of every access is archived and accessible centrally within the ÚZČ;
- interception is activated by the ÚZČ – Center of information systems. The center cannot edit the request and does not have access to the intercepted records.

The Czech Republic is experimenting with the electronic criminal file in order to make the criminal procedure more efficient. The whole system is governed by the general law governing criminal procedure and also by the special bylaws governing the filing system – mainly the Instruction of the Ministry of Justice No. 505/2001-Org on Interior and Office Regulation for district, regional, and higher courts. Theoretically, once the electronic filing system is fully implemented, the criminal procedure can be conducted electronically as a whole and, at that point, a real-time transfer mechanism can be implemented. At this time, the electronic filing system of the Czech police is accessible to the prosecution by guaranteed and secured connection through the centralized communication infrastructure. This partial cooperation was made possible by the Order of the Police President No. 125/2008, but full-scale digitisation is still to be achieved.

Additional technical regulation is provided by the Czech Act No. 412/2005 Sb. on the Protection of Classified Information.[182] The Czech police constantly argues that, according to Section 65 of Act No. 141/1961 Sb., the obtained communication data are classified, possessing the "confidential" secrecy level.

Section 65 Code of Criminal Procedure

(1) The accused, victim and party to an action, their defence counsel and their agents have the right to inspect files, with the exception of the voting record and the personal

[182] Available in English at http://www.nbu.cz/en/legislation/

data of the witnesses in accordance with Section 55 Subsection 2, to make extracts from them and notes, and make copies of files and their parts at own expense. The same right applies to the legal representatives of the accused, victim or the party to an action if they are denied legal capacity or if their legal capacity is restricted. Other people may then do so with the consent of the presiding judge and in criminal proceedings with the consent of the public prosecutor or the police authority only if it is necessary to exercise their rights.

(2) The public prosecutor or the police authority are entitled to inspect the files, along with the other rights referred to in Subsection 1, and they may deny them based on important reasons in the preliminary hearing. The public prosecutor is obligated to urgently review the severity of the grounds on which those rights are denied by the police authority and the request of the person to whom the refusal concerns. These rights can not be denied to the accused and the defence counsel once they have been advised of the possibility to study the files, and when concluding an agreement on guilt and punishment.

(3) Those who had the right to be present to an action can not be denied access to the transcript of such an action. The accused and their legal counsel could not be denied access to the resolution to initiate criminal prosecution (Section 160 Subsection 1).

(4) The rights of public authorities to access the files under other legal regulations are not established with prejudice to the provisions of the preceding Subsections.

(5) When authorising access to the files, it is necessary to take such steps to preserve the secrecy of the classified information protected by a special Act which is related to the state ordered or recognised confidentiality obligation.

According to the Czech police, the request to maintain secrecy also covers the intercepted communication data, because of its protection by law. This interpretation is criticized by some police officers and public prosecutors; however, the current practice is most likely not going to change within the foreseeable future due to lack of political will at police headquarters.

4. Real-time transfer of communication data

As mentioned above, intercepted communication can be transferred in real-time or subsequently according to Art. 18 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, which has application priority over national law. However, based on individual consultations, it appears that the Czech Republic is poorly prepared for such a real-time solution and subsequent transfers are generally used.

Art. 19 of the Convention regarding access to communication providers also takes priority in application, but intercepted communication cannot be transferred without the involvement of a domestic authority.

C. European Investigation Order

Based on individual interviews with police officers and public prosecutors, only minor adjustments are expected. Moreover, the Czech government has not issued any official statement regarding the European Investigation Order so far.

D. Statistics

Complete statistics regarding the number of warrants for electronic communication interceptions are, unfortunately, unavailable. For the sake of secrecy and the confidentiality of investigation, the available statistics do not contain the absolute number of interceptions but only the number of police files in which electronic communication interception was enacted. In the last several years, the number of police files containing interception for mutual legal assistance has been consistently low.

In 2011,[183] there was one police file containing an interception at the the regional police headquarters level[184] and five police files containing interceptions in nationwide units.[185] The total number of files with electronic communication interceptions was 731 at the regional level and 206 at the national level.

In 2012,[186] the number of police files with electronic communication interceptions rose to 1120 at the national level, but none of them contained interception warrants based on mutual legal assistance. Within the nationwide units, there were 240 files with interception but only six stemming from mutual legal assistance.[187]

In 2013,[188] only three[189] of 1175 files at the regional level contained electronic communication interceptions based on mutual legal assistance. On a nationwide scale, there were three[190] of 226 files.

---

[183] Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2011. Praha, 2012. 176 p. Available at http://www.mvcr.cz/soubor/ppr-2261-13-cj-2012-0099ta-analyza-2012-final-ver-pdf.aspx. p. 58.

[184] Region of Ústí na Labem.

[185] 2 for Útvar pro odhalování organizovaného zločinu [Organised Crime Unit], 1 for Národní protidrogová central [National Anti-drug Unit], 1 for Úřad služby kriminální policie a vyšetřování [Criminal and Investigation Unit] and 1 for Útvar pro odhalování korupce a finanční criminality [Corruption and Financial Crimes Unit].

[186] Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2012. Praha, 2013. 151 s. http://www.mvcr.cz/soubor/analyza-odposlechu-a-zaznamu-pdf.aspx. p. 54.

[187] 3 for Úřad služby kriminální policie a vyšetřování [Criminal and Investigation Unit], 2 for Útvar pro odhalování organizovaného zločinu [Organised Crime Unit], 1 for Národní protidrogová central [National Anti-Drug Unit].

[188] Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2013. Praha, 2014. 140 p. Available at http://www.mvcr.cz/soubor/ppr-102-31-cj-2014-990390-analyza-odposlechu-a-sledovani-za-rok-2013-pdf.aspx. p. 48.

[189] 2 for region Ústí nad Labem and 1 for the capital of Prague.

[190] 2 for Útvar pro odhalování organizovaného zločinu [Organised Crime Unit], 1 for Národní protidrogová central [National Anti-drug Unit].

Bibliography*

Analýza odposlechů a záznamů telekomunikačního provozu a sle-dování osob a věcí dle trestního řádu a rušení provozu elektro-nických komunikací Policií ČR za rok 2013. Praha, 2014. Available at http://www.mvcr.cz/soubor/ppr-102-31-cj-2014-990390-analyza-odposlechu-a-sledovani-za-rok-2013-pdf.aspx

Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2011. Praha, 2012. Available at http://www.mvcr.cz/soubor/ppr-2261-13-cj-2012-0099ta-analyza-2012-final-ver-pdf.aspx

Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2012. Praha, 2013. Available at http://www.mvcr.cz/soubor/analyza-odposlechu-a-zaznamu-pdf.aspx

Čičkánová, D., Procesnoprávne aspekty práva na informačné sebaurčenie a práva byť zabudnutý. Bratislavské právnické fórum 2013. Bratislava: Univerzita Komenského, Právnická fakulta, 2013.

Minarik, Š., Trestný poriadok. Komentár. Iura edition, spol. s r.o. 2010, Bratislava

Myška, M. Právní aspekty uchovávání provozních a lokalizačních údajů. Brno : Masarykova univerzita, 2013.

Novotná, J., Právní pomoc v cizím státu v přípravném řízení trestním. 3. vydání. Praha : C.H. Beck, 2015.

Polčák, R., Harašta, J., Stupka, V. Právní problémy kybernetické bezpečnosti. Brno : Masarykova univerzita, 2016.

Polčák, R., Púry, F., Harašta, J. Elektronické důkazy v trestním řízení. Brno : Masarykova univerzia, 2015.

Šámal, P., Odposlech a záznam telekomunikačního provozu ve světle judikatúry. Soudní rozhledy, C.H. Beck. 2000.

Šámal, Pavel, Trestní řád: komentář. 7., extended release. In Prague: C.H. Beck, 2013, Velké komentáře.

Vantuch, P., Nová úprava odposlechu v trestním řádu od 1. 7. 2008. Bulletin advokacie, 2008

List of Abbreviations

ASPI	Automated legal information system
Cell ID	Cell Identification
CERT	Computer Emergency Response Team

* All URLs were last accessed in 9/2018.

EMS	Enhanced media service
ENISA	European Network and Information Security Agency
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet protocol
ISP	Internet service provider
ITM	Information and Technical Mean
ITP	Information and Technical Procedure
MAC adress	Media access control address
MLA	Mutual Legal Assistance
MMS	Multimedia Messaging Service
Sb.	Sbírka zákonů (Collection of Law)
Sb. m. s.	Sbírka mezinárodních smluv (Collection of international treaties)
SFTP	Secure File Transfer Protocol
SHA-1	Secure Hash Algorithm 1
SIM	Subscriber identity module
SMPT	Simple Mail Transfer Protocol
SMS	Short Message Service
spis. zn.	Spisová značka (case number)
ÚZČ	Útvar zvláštních činností (Unit for Special Activities of Criminal Police and Investigation)
VoIP	Voice over IP
ZMJS	Zákon o vzájemné justiční spolupráci ve věcech trestníc (Act No. 104/2013 Sb. on Mutual Judicial Assistance in Criminal Matters)

Estonia*

National Rapporteur:
Aare Kruuser

* This report reflects legislation and case law as of March 2019.

Contents

I. General Background of the National Legal System of the Republic of Estonia

A. Basic Architecture of the Legal System

Estonia is part of the Continental European legal system (civil law system). According to the classic approach, the Estonian legal system belongs to the continental European legal tradition, to the Roman-Germanic family, and follows the classic division into private, public, and criminal law. Since the Estonian legal system was rapidly developed, after the country regained independence, many different countries and legal systems were taken as examples, as well as generally recognized principles of international law, binding international treaties and European Union legal acts which form an inseparable part of Estonian law.

In order to characterize the Estonian legal system it is been necessary to note that judicial precedent also serves as a source of law in Estonia, as for a system governed by rule of law (the Estonian legal system is formally norm-based, not a mix of precedent and statutory law) legal gaps should not exist and the interpretation of law is important in a changing society. In the wider meaning case law has no precedent value, but the decisions of the Estonian Supreme Court are used as a subsidiary source of law in interpreting and founding the general principles of law. This follows expressis verbis from the Estonian Code of Criminal Procedure (ECCP), which states in § 2 subsection 4 that the decisions of the Supreme Court on issues which are not regulated by other sources of criminal procedural law (the Constitution of the Republic of Estonia; the generally recognized principles and provisions of international law and international agreements binding on Estonia; this Code and other legislation which provides for criminal procedure) but which arise in the application of law are also sources of criminal procedure law.[1] In practice the decisions of the Supreme Court on issues which are not regulated by other sources of law are de facto also sources of law in other areas of law: private law, and in particular administrative law.

B. Sources of Law

The basic architecture of the legal system of the Republic of Estonia is described on the European e-Justice Portal[2] as follows:

---

[1] For the text and translation into English of the Act, please see annex.

[2] https://e-justice.europa.eu/content_member_state_law-6-ee-en.do?member=1

The most important sources of law in Estonia are legal instruments such as the Constitution, European Union law, international agreements, Acts and Regulations. Legal interpretations given by the highest court – the Supreme Court – and comments by experts also serve as reference points.

Court judgments do not create rights, and in general judgments handed down by higher courts are not binding on lower courts. However, the Supreme Court, which is also the court of constitutional review, is authorised to declare legal instruments invalid if they are not in accordance with the Constitution or with legal instruments taking precedence over them. When addressing particular cases, no court may apply such an instrument, and the courts are authorised not to apply any legal instrument that is in conflict with the Constitution. The Supreme Court, as the court of constitutional review, then examines the case further and is authorised to declare any such instrument unconstitutional (but not invalid).

Generally recognised principles and rules of international law are an inseparable part of the Estonian legal system.

1. Types of legal instruments

– *Constitution* – in accordance with § 3(1) Constitution, state authority is exercised solely pursuant to the Constitution and Acts which are in conformity with it.

– *Acts* – in accordance with § 65 Constitution, Acts are adopted by the Estonian Parliament (the *Riigikogu*), in which legislative power is vested. Acts are adopted in accordance with the Constitution and are published in the prescribed manner in the State Gazette *(Riigi Teataja)*. Only Acts that have been published are enforceable.

– *Regulations* – in accordance with §§ 87 and 94 Constitution, the Government of the Republic and Ministers are authorised to issue Regulations on the basis of and for the purpose of complying with an Act. In order to deal with issues of local importance or in cases laid down in an Act, local government councils are also authorised to issue Regulations. A Regulation is, in essence, a basic act. Regulations may be issued only on the basis of a limited scope of authority laid down in an Act. In addition to the Government of the Republic, the right to issue Regulations has also been granted to other independent legal entities – legal persons in public law (universities) and public bodies. Furthermore, on the basis of § 154(1) Constitution local government councils are also authorised to issue Regulations, as is the Bank of Estonia *(Eesti Pank)* on the basis of § 111.

Regulations enter into force on the third day following their publication in *Riigi Teataja*, except as otherwise provided in the Regulation.

– *Administrative Orders* – an individual administrative act by which a public-law administration decides on and organises individual legal issues. In accordance

with § 87(6) Constitution, the Government of the Republic issues Administrative Orders on the basis of and for compliance with an Act. The Prime Minister, county governors and local governments are also authorised to issue Administrative Orders.

– *Decisions* – an individual administrative act issued on the basis of administrative challenges or appeals or by which sanctions are imposed. Decisions are also adopted by Parliament, local government councils, the National Electoral Committee and the courts.

– *Orders* – in accordance with § 94 Constitution, Ministers issue Orders on the basis of and for compliance with an Act. An Order includes a general mandatory code of conduct for issues relating to service in a Ministry or for determining the structure and organising the operations of State bodies operating under the jurisdiction of a Ministry.

– *International agreements and the primacy of European Union law* – in accordance with § 3(1) Constitution, generally recognised principles and rules of international law are an inseparable part of the Estonian legal system. § 123 Constitution states that the Republic of Estonia does not enter into international agreements that are in conflict with the Constitution. The Act amending the Constitution lays down the principle of the primacy of European Union law. Pursuant to § 2 of that Act, while Estonia is a member of the European Union the Estonian Constitution applies, having regard to the rights and obligations under the Act of Accession. If Estonian Acts or other legal instruments are in conflict with international agreements ratified by Parliament, the provisions of the international agreement apply.

International agreements enter into force in accordance with the procedure laid down in the agreements.

The application of foreign law is regulated by the Private International Law Act. If foreign law is to be applied under an Act, international agreement or transaction, it is applied by a court irrespective of whether an application to that end has been made. Foreign law is applied in accordance with its interpretation and application in practice in the country concerned. Foreign law is not applied if the result would be a clear contradiction with the fundamental principles of Estonian law (public order). In such cases, Estonian law is applied.

– *Decrees* – under § 109 Constitution, if it is impossible to convene Parliament, the President of the Republic may, in the event of urgent national need, issue Decrees having the force of law. Such Decrees must be countersigned by the President (speaker) of the Parliament and the Prime Minister.

Under the Constitution, the President may issue:

– special Decrees in the event of urgent national need and if it is impossible to convene Parliament;

– emergency Decrees in the event of urgent national need, where the Government has declared a state of emergency and if it is impossible to convene Parliament or there is not enough time for Parliament to be convened.

A Decree issued by the President of the Republic enters into force on the tenth day following its publication in *Riigi Teataja*, except otherwise provided in the Decree.

Once Parliament has convened, the President of the Republic lays the Decrees before Parliament, which then promptly adopts an Act to approve or repeal them. Under § 110 Constitution, the President of the Republic may not use a Decree to enact, amend or repeal the Constitution, the Acts referred to in § 104 Constitution, Acts setting national taxes or the State budget.

2. Hierarchy of legal instruments

The hierarchy of legal instruments is as follows: the Constitution, European Union law, international agreements, Acts and Decrees, Government of the Republic Regulations and Regulations issued by Ministers. Besides basic legal acts, there are also individual acts that are issued on the basis of an Act and are located in the hierarchy below Acts and Regulations. The legal instruments at each level must be in accordance with those at a higher level.

3. Publication of legal instruments

The most important legal instruments and international agreements are published in *Riigi Teataja*. Acts and Regulations gain legal force only once they have been published in *Riigi Teataja*.

Riigi Teataja is Estonia's official online publication and the central database of legal instruments. Since 1 June 2010 *Riigi Teataja* has been published only on the internet, as an official online publication. Since 1 January 2011, *Riigi Teataja* has been published by the Ministry of Justice. Various news items relating to Acts and the law in general are also published in *Riigi Teataja*.

In 2011 sworn translators began providing English translations of the updated texts of Acts, a process that was organised by the Ministry of Justice. On 30 October 2013 the *Riigi Teataja* website in English was launched. This contains updated English translations of the consolidated texts of Although the translations do not have legal force they are kept updated, and the translations of amendments are generally added to the consolidated texts before the amendments enter into force. Anyone can have the latest translations sent to their e-mail address by signing up for the My RT service.

Access to *Riigi Teataja* and to all legal information services is free of charge for users.

C. The Legal Basis for the Estonian Judicial System and Rules of Court Procedure

The legal basis for the Estonian judicial system and rules of court procedure are:
- Constitution of the Republic of Estonia (adopted by referendum on 28 June 1992);
- Courts Act (in force since 29 July 2002);
- internal rules of the courts.

Rules of court procedure are provided by:
- Code of Civil Procedure;
- Code of Criminal Procedure;
- Code of Administrative Court Procedure;
- Code of Misdemeanour Procedure;
- Constitutional Review Proceedings Act.

The following summary is based on legal acts regulating the topic and their public translations into English.

II. Constitutional, Legal, and Doctrinal Safeguards for the Interception of Electronic Communications

A. Specific Constitutional and Non-Constitutional Protection for Electronic Communications and for Computer-Stored Data

Estonia has constitutional, legal, and doctrinal safeguards for the protection of telecommunications data. § 43 Constitution[3] stipulates that everyone has the right to confidentiality of messages sent or received by them by post, telegraph, telephone or other commonly used means. Derogations from this right may be made in certain cases pursuant to a procedure provided by law if they are authorized by a court and if they are necessary to prevent a criminal offence, or to ascertain the truth in a criminal case.

The constitutional "principle of proportionality and necessity" is provided as the criminal proceedings must be guided by the principle of expediency and proportionality for any action that has already been taken, and for the use of interception of electronic communications, the ultima ratio principle is explicitly stated in criminal procedure. The request must be justified in any case and a query may be executed only if this is indispensable for the purpose of the criminal proceedings.

---

[3] For the text and translation into English of the Act, please see annex.

According to § 26 Constitution, a person's family and private life may be interfered with only in the event and in the manner prescribed by law for the protection of health, morals, public order or the rights and freedoms of others, for the prevention of a criminal offence or for the capture of an offender.

According to §§ 9–11 and 13–15 Constitution, the rights, freedoms, and duties of all persons and of everyone, as set out in the Constitution, apply equally to citizens of Estonia and to citizens of foreign states and stateless persons in Estonia.

The rights, freedoms, and duties set out in the Constitution extend to legal persons in so far as this is in accordance with the purpose of legal personality and with the nature of such rights, freedoms, and duties.

The rights, freedoms, and duties set out in the Constitution do not preclude other rights, freedoms, and duties which arise from the spirit of the Constitution or are in accordance therewith, and which are in conformity with the principles of human dignity, social justice, and democratic government founded on the rule of law.

Rights and freedoms may only be circumscribed in accordance with the Constitution. Such circumscription must be necessary in a democratic society and may not distort the nature of the rights and freedoms circumscribed.

Everyone is entitled to protection by the government and of the law. The Estonian government also protects its citizens abroad. The law protects everyone from arbitrary exercise of governmental authority.

It is the duty of the legislature, the executive, the judiciary, and of local authorities, to guarantee the rights and freedoms provided in the Constitution. Everyone whose rights and freedoms have been violated has the right of recourse to the courts. Everyone is entitled to petition the court that hears his or her case to declare unconstitutional any law, other legislative instrument, administrative decision or measure which is relevant in the case. The courts observe the Constitution and declare unconstitutional any law, other legislative instrument, administrative decision or measure which violates any rights or freedoms provided in the Constitution or which otherwise contravenes the Constitution.

There are also legal safeguards to ensure effective protection of the intercepted data against the risk of abuse and against any unlawful access and use of that data. § 9 subsection 4 Code of Criminal Procedure provides that in a criminal proceeding, it is permitted to interfere with the private and family life of a person only pursuant to the procedure provided for in this Code, in order to prevent a criminal offence, apprehend a criminal offender, ascertain the truth in a criminal matter or secure the execution of a court judgment.

The State Secrets and Classified Information of Foreign States Act[4] stipulates in § 20 (1), that the person in possession of classified information is required to adopt suitable organizational, physical, and INFOSEC[5] security measures for the protection of state secrets. The purpose of this Act is to ensure the security and foreign relations of the Republic of Estonia, protecting state secrets and classified information of foreign states from disclosure and becoming accessible to persons who have not been granted access to such information. Estonian State Secrets and Classified Information of Foreign States Act (ESSCIFSA) provides the definition of information which is classified as a state secret, grounds for the expiry of a classification notice for state secrets and classified information of foreign states, and the basis for classification and the changing of related terms; the grounds for the protection of state secrets, classified information of foreign states and classified media and liability incurring from the violation of this Act. The above-mentioned interception of electronic communications activities and most matters relating to the interception of electronic communications in the above-mentioned fields are treated as state secrets related to the maintenance of law and order, to national defence, to foreign relations, to security authorities, to infrastructure and protection of information, etc., i.e., that the data collected may be used only in compliance with the goals and according to the procedure provided by law.

§ 35 ESSCIFSA provides that internally, state secrets communicated to a possessor of classified information may only be communicated upon the written consent of a head or directing body of an agency, constitutional institution, or public legal person that is the originator of the state secret or, in the case of a state secret related to criminal proceedings, the prosecutor in charge of the proceedings or a prosecutor above him, observing the procedure specified in this Act and legislation issued on the basis thereof. If a natural person outside a service or a legal person governed by private law is an originator of the information, an agency supporting the granting of a Personnel Security Clearance or a Facility Security Clearance shall also give written consent for communication of the information. The consent is not needed if a ministry communicates a state secret at the confidential or lower level to an agency within the area of government of the respective ministry. Provisions of § 35 subsection 1 and 2 ESSCIFSA shall not apply to the communication of state secrets within an agency, constitutional institution or legal person, also when communicating state secrets to authorities, specified in §§ 22 and 23 of this Act, i.e., the National Security Authority, a court, the *Riigikogu*, the Chancellor of Justice, the Auditor General, the Government of the Republic, and, in the case provided for in subsection 10 (2) of the Security Authorities Act, to relevant governmental authorities and the President of the Republic.

---

[4] For the text and translation into English of the Act, please see annex.

[5] "INFOSEC" (Information Security) means the ensuring of the availability, confidentiality and integrity of state secrets or classified information of foreign states in the automated systems processing state secrets or classified information of foreign states.

State secrets may be communicated to a foreign state, international organisation or an institution established under an international agreement by the Government Office, Ministry of Defence, Ministry of the Interior, Ministry of Foreign Affairs, the Defence Forces, and a security authority in the procedure provided for in this Act and legislation issued on the basis thereof if this is necessary to ensure or increase the security of the Republic of Estonia under an international agreement and if the agency receiving the information ensures the protection of the communicated information from disclosure. State secrets may be communicated to a foreign state, international organisation, or an institution established under an international agreement by the Police and Border Guard Board, observing the procedure specified in this Act and legislation issued on the basis thereof and the provisions of the Witness Protection Act, provided that the agency receiving the information ensures the protection of communicated information from disclosure. State secrets containing surveillance information at the 'restricted' level that is required for the maintenance of law and order may be communicated to a foreign state, international organisation, or an institution established under an international agreement by a competent surveillance authority or the Prosecutor's Office if such obligation is due under European Union law or an international agreement, or is required for the work of an international investigation group, provided that the agency receiving the information ensures the protection of the communicated information from disclosure. Communication of state secrets to a foreign state, international organisation or an institution established under an international agreement must first be registered at the National Security Authority, except if information is being communicated by a security authority under the conditions provided for in this section, if information specified in § 35 clauses 7 5^{1}), 7), 10) and 11) ESSCIFSA is communicated by the Defence Forces to a foreign state or if information is communicated under § 35 subsections 5 or 5^{1} ESSCIFSA.

§ 36 ESSCIFSA provides that maintaining records of classified media is performed as provided by the Administrative Procedure Act, the Archives Act, a regulation of the Government of the Republic, adopted under subsection 58 (1) Public Information Act and the legislation issued on the basis thereof, considering the specifications provided for by this Act and the legislation issued on the basis thereof. Registration of copies made of classified media, except the media containing state secrets classified as 'restricted' or 'confidential,' is mandatory. The Government of the Republic may lay down requirements different from the provisions specified in § 36 subsection 2 ESSCIFSA for the registration of electronic classified media, observing the Procedure for Protection of State Secrets and Classified Information of Foreign States.

B. Principles for the Definition of Coercive Powers in Criminal Procedural Law

There are constitutional and doctrinal rules for the precise definition or interpretation of coercive powers in criminal procedural law (such as the *nullum crimen sine lege* principle in substantive criminal law,[6] as well the principle of precise parliamentary enactment of public powers).[7]

According to §§ 17, 18, 20–22, 59, and 146 Constitution no one may be convicted of an act which did not constitute a criminal offence under the law in force at the time the act was committed.

Legislative authority is vested in the *Riigikogu*. Justice is administered exclusively by the courts. The courts are independent in discharging their duties and administer justice in accordance with the Constitution and the laws.

No one may be deprived of his or her liberty except in the cases and pursuant to a procedure provided by law:

1) to enforce a judgment of conviction rendered or a detention ordered by a court;
2) in the case of non-compliance with a direction of a court, or to guarantee fulfilment of a duty provided by law;
3) to prevent a criminal or administrative offence, to bring before a competent authority a person in relation to whom there is reasonable suspicion that he or she has committed such an offence, or to prevent such a person from absconding;
4) to place a minor under disciplinary supervision or to bring him or her before a competent authority to determine whether to impose such supervision;
5) to detain a person suffering from an infectious disease, a person of unsound mind, an alcoholic or a drug addict, if such a person poses a danger to himself or herself or to others;
6) to prevent illegal settlement in Estonia and for removing a person from Estonia or for extraditing a person to a foreign state.

No one may be deemed guilty of a criminal offence before he or she has been convicted in a court and before the conviction has become final.

No one is required to prove his or her innocence in criminal proceedings.

Everyone is entitled to compensation for intangible as well as tangible harm that he or she has suffered because of the unlawful actions of any person.

An analogous application of coercive powers in criminal procedure is not possible.

---

[6] In substantive criminal law, the principle "no crime without legal definition" requires inter alia that criminal statutes be defined precisely by the legislator before the commission of a criminal act can be assumed.

[7] The principle of precise parliamentary enactment of public powers requires that all infringements of civil liberties be based on precise laws.

Every person suspected or prosecuted is presumed innocent as long as guilt has not been established. Attacks on his presumption of innocence are proscribed, compensated for, and punished in the circumstances laid down by statute. Everybody has the right to be informed of charges brought against him and to be legally defended. Investigations into serious crimes are frequently associated with court approval for coercive measures and see prosecutorial involvement as guaranteeing the quality of investigation. The coercive measures to which such a person may be subjected are taken by or under the effective control of judicial authority. They should be strictly limited to what is necessary for the process, proportionate to the gravity of the offence charged and not such as to infringe human dignity. The accusation to which such a person is subjected should be brought to judgment within a reasonable time. Every convicted person has the right to have his conviction examined.

C. Liability in the Estonian State Secrets and Classified Information of Foreign States Act

The law includes specific safeguards in this sphere.

1. Violation of requirements to protect state secrets

§ 53 ESSCIFSA provides that violation of requirements to protect state secrets by a person holding the right of access to state secrets if accompanied by danger of disclosure or becoming known to a person with no right of access, processing of information as state secrets with no legal grounds, classification of state secret on the incorrect legal grounds, at an incorrect level or for an incorrect term, failure to classify a state secret, failure to declassify a state secret after the lapse of a threat to security before the expiry of classification term or failure to comply with the notification requirement, specified in subsections 19 (3), (4), (6), and (7), subsection 32 (4), subsection 42 (6) or § 45 ESSCIFSA shall be punishable by a penalty fine of up to 200 fine units[8] or an arrest.

The conduct specified in § 53 subsection 1 ESSCIFSA shall be punishable by a penalty fine of up to 300 fine units or an arrest, if the object of a misdemeanour is a state secret classified as ‘secret’ or ‘top secret.’ If committed by a legal person, the conduct specified in § 53 subsections 1–2 ESSCIFSA of this section shall be punishable by a penalty fine of up to 32,000 euros.

[8] A fine unit is the base amount of a fine and is equal to 4 euros.

2. Disclosure of state secrets due to negligence and loss of a classified medium

§ 54 ESSCIFSA provides that disclosure, unlawful communication or allowing unlawful access to state secrets by a person required to maintain the confidentiality of state secrets, if the conduct was due to negligence and also the loss of a classified medium, shall be punishable by a penalty fine of up to 300 fine units or an arrest. The same act if committed by a legal person shall be punishable by a penalty fine of up to 32,000 euros.

3. Liability for violation of ESSCIFSA

§ 55 ESSCIFSA provides that a person shall not be relieved from responsibility when committing a misdemeanour, the object of which was a state secret, information was declassified or the legal grounds, classification level or term for classification of such information was changed, except if there were no legal grounds for the classification of such information. A person shall be responsible for classification of information with no legal grounds also after the declassification of such information.

If a person is deprived of the right of access to a state secret and classified information of a foreign state or the right for processing state secrets and classified information of a foreign state outside the immovable or a movable possessed by a state agency or *Eesti Pank* for the commitment of a misdemeanour under the State Secrets and Classified Information of Foreign States Act, such person must apply again for the respective right for a Personnel Security Clearance or a Facility Security Clearance to obtain the right of access or processing right.

Provisions of the general part of the Penal Code and the Code of Misdemeanour Procedure shall be applicable to the misdemeanours specified in this chapter. Extrajudicial proceedings in a misdemeanour specified in this chapter shall be conducted by the Internal Security Service.

D. Liability in the Estonian Penal Code

Unlawful surveillance activities and covert collection of information, removal and fraudulent creation of evidence and unlawful disclosure of information concerning pre-trial proceedings in criminal matters and surveillance proceedings are crimes in Estonia.

1. Unlawful surveillance activities and covert collection of information

§ 315 Penal Code[9] provides that unlawful surveillance activities or unlawful and covert collection of information, unlawful concealment or destruction of information collected by surveillance activities or covertly, if conducted by a person with the right arising from law to engage in surveillance or covert collection of information, is punishable by a pecuniary punishment or up to three years' imprisonment. The same act, if committed by a legal person, is punishable by a pecuniary punishment.

2. Removal and fraudulent creation of evidence

§ 316 Penal Code provides that removal or fraudulent creation of evidence with the intention of obstructing ascertainment of the commission or absence of an act punishable as a criminal offence, or of any other facts relating to the subject of proof, is punishable by a pecuniary punishment or by one to five years' imprisonment. The same act, if committed by a legal person, is punishable by a pecuniary punishment.

3. Unlawful disclosure of information concerning pre-trial proceedings in criminal matters and surveillance proceedings

§ 316[1] Penal Code provides that unlawful disclosure of information relating to pre-trial proceedings in a criminal matter or information relating to surveillance proceedings carried out in order to prevent or combat a criminal offence by a person who became aware of such information in connection with the performance of his or her employment duties or functions, resulting in the impossibility or significant complication of the establishment of the existence or absence of an act subject to punishment as a criminal offence, or establishment of other facts of the subject of proof, or achievement of the aim of surveillance activities is punishable by a pecuniary punishment or up to five years' imprisonment. The same act, if committed by a legal person, is punishable by a pecuniary punishment.

---

[9] For the text and translation into English of the Act, please see annex.

III. Coercive Powers for Accessing Electronic Communications Data

A. Overview of the Legal Framework and the Respective Provisions: Framework for Accessing Electronic Communications Data

1. Regulatory framework for retention of data and granting access to electronic communications

The key law that regulates the communications sector is the Estonian Electronic Communications Act[10] (EECA), passed on 8 December 2014 and entered into force 1 January 2005. The purpose of EECA is to create the necessary conditions for the development of electronic communications to promote the development of electronic communications networks and electronic communications services without giving preference to specific technologies and to ensure the protection of the interests of users of electronic communications services by promoting free competition and the purposeful and just planning, allocation, and use of radio frequencies and numbering.

EECA provides requirements for the public electronic communications networks and publicly available electronic communications services, for the use of electronic contact details for direct marketing, for the conduct of radiocommunication, for the management of radio frequencies and numbering, and for radio equipment as well as state supervision over the compliance with these requirements and liability for the violation of these requirements.

The EECA does not apply to information society services within the meaning of the Information Society Services Act, unless otherwise provided by EECA. The provisions of the national Administrative Procedure Act apply to the administrative proceedings prescribed in EECA, taking account of the specifications provided for in EECA.

According to § 2 EECA:

1) local sub-loop means the physical circuit connecting the termination point to an intermediate distribution point in a fixed electronic communications network;
2) electromagnetic compatibility means the capability of radio equipment to satisfactorily function in an electromagnetic environment without causing electromagnetic interference to other equipment located in that environment;
3) electronic communications undertaking (hereinafter *communications undertaking*) means a person who provides publicly available electronic communications

[10] For the text and translation into English of the Act, please see annex.

services to the end-user or to another provider of publicly available electronic communications services;

4) electronic communications service means a service which consists wholly or mainly in transmission or conveyance of signals over the electronic communications network under the agreed conditions. Network services are also electronic communications services;

5) user of electronic communications services (hereinafter *user of communications services*) means a person using publicly available electronic communications services;

6) electronic communications network means a transmission system including switching equipment and other support systems for the transmission or conveyance of signals by way of a cable or by radio, optical or other electromagnetic means. Electronic communications networks include also the satellite network, telephone network, data communication network, mobile telephone network, broadcasting network, cable network, and electric cable system, if used for the transmission or conveyance of signals, regardless of the nature of information transmitted over such networks;

7) electronic contact details mean details which enable the conveyance of information to a person over electronic communications networks, including by fax, electronic mail, SMS or MMS messages.

2. Obligation to preserve data

§ 111^1 EECA validates the obligation to preserve data for electronic communications undertakings (hereinafter *communications undertaking*, means a person who provides publicly available electronic communications services to the end-user or to another provider of publicly available electronic communications services). According to the EECA a communications undertaking is required to preserve the data that is necessary for the performance of the following acts:

1) tracing and identification of the source of communication;

2) identification of the destination of communication;

3) identification of the date, time and duration of communication;

4) identification of the type of communications service;

5) identification of the terminal equipment or presumable terminal equipment of a user of communications services;

6) determining of the location of the terminal equipment.

The providers of telephone or mobile telephone services and telephone network and mobile telephone network services are required to preserve the following data:

1) the number of the caller and the subscriber's name and address;

2) the number of the recipient and the subscriber's name and address;

3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialled and the subscriber's name and address;
4) the date and time of the beginning and end of the call;
5) the telephone or mobile telephone service used;
6) the international mobile subscriber identity (IMSI) of the caller and the recipient;
7) the international mobile equipment identity (IMEI) of the caller and the recipient;
8) the cell ID (cell ID means an identifier which shows from which cell the mobile telephone service has been originated or to which cell it has been terminated) at the time of setting up the call;
9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data is preserved;
10) in the case of anonymous prepaid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated.

The providers of Internet access, electronic mail, and Internet telephony services are required to preserve the following data:

1) the user ID allocated by the communications undertaking;
2) the user ID and telephone number of any incoming communication in the telephone or mobile telephone network;
3) the name and address of the subscriber to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;
4) the user ID or telephone number of the intended recipient of an Internet telephony call;
5) the name, address, and user ID of the subscriber who is the intended recipient in the case of electronic mail and Internet telephony services;
6) the date and time of beginning and end of the Internet session, based on a given time zone, together with the IP address allocated to the user by the Internet service provider and the user ID;
7) the date and time of the log-in and log-off of the electronic mail service or Internet telephony service, based on a given time zone;
8) the Internet service used in the case of electronic mail and Internet telephony services;
9) the number of the caller in the case of dial-up Internet access;
10) the digital subscriber line (DSL) or other endpoint of the originator of the communication.

The data specified in § 111^1 subsections 2 and 3 EECA shall be preserved for one year from the date of the communication if such data is generated or processed

in the process of provision of communications services. Requests submitted and information given pursuant to § 112 EECA shall be preserved for two years. The obligation to preserve the information provided pursuant to § 112 EECA rests with the person submitting the request. The data specified in § 111^1 subsections 2 and 3 EECA shall be preserved in the territory of a Member State of the European Union. The following shall be preserved in the territory of Estonia:

1) the requests and information provided for in § 112 EECA;
2) the log files specified in § 113 subsection 5 EECA and the applications provided for in § 113 subsection 6 EECA;
3) the single requests provided for in § 114^1 EECA.

In the interest of public order and national security the Government of the Republic may extend, for a limited period, the term specified in § 111^1 subsection 6 EECA. If this is carried out, the minister responsible for the area shall immediately notify the European Commission and the Member States of the European Union. In the absence of an opinion of the European Commission within a period of six months the term specified in § 111^1 subsection 4 EECA shall be deemed to have been extended.

The obligation to preserve the data also applies to unsuccessful calls if this data is generated or processed upon providing telephone or mobile telephone services or telephone network or mobile telephone network services. The specified obligation to preserve data does not apply to call attempts.

Upon preserving the data specified in § 111^1 subsections 2 and 3 EECA, a communications undertaking must ensure that:

1) the same quality, security, and data protection requirements are met as those applicable to analogous data on the electronic communications network;
2) the data is protected against accidental or unlawful destruction, loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;
3) necessary technical and organisational measures are in place to restrict access to the data;
4) no data revealing the content of the communication is preserved.

Communications undertakings will not be compensated for the expenses relating to the preservation or processing of the data specified in § 111^1 subsections 2 and 3 EECA.

The data specified in § 111^1 subsections 2 and 3 EECA is forwarded to:

1) an investigative body, a surveillance agency, the Prosecutor's Office or a court pursuant to the Code of Criminal Procedure;
2) a security authority;
3) the Data Protection Inspectorate, the Financial Supervision Authority, the Environmental Inspectorate, the Police and Border Guard Board, the Estonian Inter-

nal Security Service, and the Tax and Customs Board pursuant to the Code of Misdemeanour Procedure;

4) the Financial Supervision Authority pursuant to the Securities Market Act;

5) a court pursuant to the Code of Civil Procedure;

6) a surveillance agency in the cases provided for in the Organisation of the Defence Forces Act, the Taxation Act, the Police and Border Guard Act, the Weapons Act, the Strategic Goods Act, the Customs Act, the Witness Protection Act, the Security Act, the Imprisonment Act, and the Aliens Act.

The results of specific interception measures under these different regimes can be exchanged between the competent authorities within Estonia and with competent authorities in other countries.

The right to submit the request for the interception of electronic communications is also provided and regulated by the:[11]

– Code of Criminal Procedure;
– Code of Misdemeanour Procedure;
– Police and Border Guard Act;
– Security Authorities Act;
– Taxation Act;
– Customs Act;
– Witness Protection Act;
– Estonian Defence Forces Organisation Act;
– Imprisonment Act;
– Aliens Act;
– Status of Members of the Riigikogu Act;
– Security Act;
– Securities Market Act;
– Strategic Goods Act;
– Weapons Act.

3. Obligation to provide information

§ 112 EECA specifies the obligation to provide information, and states that if an agency or authority specified in previous § 111[1] subsection 11 EECA submits a request, a communications undertaking is required to provide at the earliest opportunity, but not later than ten hours after receiving an urgent request or within ten working days after receipt of the request if the request is not urgent, if adherence to

[11] For the text and translation into English of the following legal Acts, please see annex.

the specified terms is possible based on the substance of the request, the agency or authority with information concerning the data specified in § 111[1] subsections 2 and 3 EECA. The above-mentioned request shall be submitted in writing or by electronic means. Requests concerning the data specified in § 111[1] clauses (2) 1) and 2) and (3) 3) EECA may also be submitted in oral form confirming the request with a password. Access to the data specified in § 112 subsection (1) EECA may be ensured, on the basis of a written contract, by way of continuous electronic connection.

A communications undertaking providing mobile telephone services is required to provide a surveillance agency and security authority and the Police and Border Guard Board on the basis provided for in the Police and Border Guard Act with real time identification of the location of the terminal equipment used in the mobile telephone network. Access to the data specified in § 112 subsection 3 EECA must be ensured on the basis of a written contract and by way of continuous electronic connection.

4. Obligation to grant access to communications network

§ 113 EECA provides that a communications undertaking must grant a surveillance agency or security authority access to the communications network for the conduct of surveillance activities or for the restriction of the right to confidentiality of messages, correspondingly. In connection with granting access to the communications network, a communications undertaking is required to submit information concerning the technical parameters of the communications network to a surveillance agency or security authority, if they so request. Upon modification of the technical parameters of the communications network or launching of new services, a communications undertaking is required, if this may interfere with the performance of the obligations specified in § 113 subsection 3 EECA, to immediately notify the surveillance agency or security authority thereof and to commence the performance of the obligation specified in § 113 subsection 3 EECA with regard to all offered services within a reasonable period of time.

Upon granting access to the communications network, a communications undertaking is required to:

1) enable the surveillance agency or security authority to select messages and ensure their transmission to a central or portable surveillance device of the surveillance agency or security authority in an unchanged form and in real time;
2) ensure the quality of message transmission which must be equivalent to the quality of the regular services provided by the communications undertaking;
3) ensure the protection of the messages and of the data related to their transmission.

Transmission by a communications undertaking of messages to a central or portable surveillance device of a surveillance agency or security authority shall be decided by the surveillance agency or security authority. A surveillance agency or security authority shall inform the Ministry of Economic Affairs and Communications of communications undertakings who transmit messages to central or portable surveillance devices of the surveillance agency or security authority. Messages are transmitted to a central surveillance device using a message splitting interface and appropriate hardware and software, which ensures the preservation of independent log files concerning the actions by means of the central surveillance device (time, type, object, and number of action) for a period of at least five years. A communications undertaking is required to delete or destroy the log files which are older than five years and to forward to the Technical Surveillance Authority, the special security authorities surveillance committee of the *Riigikogu* and the Office of the Prosecutor General a statement which sets out the time period of creation of the deleted or destroyed log files, the time and place of their deletion or destruction, and the name, personal identification code, and position of the representative of the communications undertaking who has performed this act.

For transmission of messages to a portable surveillance device, a surveillance agency or security authority shall submit to a communications undertaking in writing or by electronic means an application for access to the communications network and set out therein the date, number, and term of validity of the authorisation of a court for the conduct of a surveillance activity or for the restriction of the right to the confidentiality of messages. The communications undertaking is required to preserve the specified applications for at least five years. A communications undertaking is required to delete or destroy the applications which are older than five years and to forward to the Technical Surveillance Authority, the special security authorities surveillance committee of the *Riigikogu*, and the Office of the Prosecutor General a statement which sets out the time period of creation of the deleted or destroyed applications, the time and place of their deletion or destruction and the name, personal identification code, and position of the representative of the communications undertaking who has performed this act.

In the event of termination of the provision of communications services by a communications undertaking, as well as upon dissolution, including as a result of a merger or division, or in the case of bankruptcy or death, the data medium containing the log files specified in § 113 subsection 5 EEC, the applications specified in § 113 subsection 6 EECA as well as the data preserved on the basis of § 111^1 and the requests submitted pursuant to § 112 EECA shall be immediately delivered to the Technical Surveillance Authority. The procedure for the preservation, delivery to the Technical Surveillance Authority, deletion and destruction of the log files, applications, data, and requests shall be established by the minister responsible for the area.

A Prosecutor's Office, in order to exercise supervision over the activities of surveillance agencies, and the special security authorities surveillance committee of the *Riigikogu*, in order to exercise supervision over the activities of surveillance agencies and security authorities, have the right to examine the applications specified in § 113 subsection 6 EECA and in the case of transmission of messages to a central surveillance device, also with the log files which are preserved. The Technical Surveillance Authority has the right to examine the log files preserved upon transmitting messages to a central surveillance device in the presence of representatives of the special security authorities surveillance committee of the *Riigikogu* and the communications undertaking in order to exercise supervision over the activities of the communications undertaking.

A communications undertaking is required to preserve the confidentiality of information related to the conduct of surveillance activities and activities which restrict the right to inviolability of private life or the right to the confidentiality of messages.

Any extraordinary unavoidable acts which are to be performed to provide access to a communications network and which interfere with the provision of communications services as well as work to be performed by a communications undertaking on the communications network which interferes with the transmission of messages to the surveillance devices shall be carried out under the conditions agreed upon between the communications undertaking and the surveillance agency or security authority in writing.

5. Compensating for costs of providing information and enabling access to communications networks

§ 114 EECA provides that a communications undertaking shall be compensated for the costs incurred in relation to the provision of the information specified in § 112 subsections 1 and 3 EECA to a surveillance agency or security authority, the enabling of access to the communications network specified in § 113 subsection 3 EECA and the transmission of messages to the surveillance device of a surveillance agency or security authority. The costs specified in § 114 subsection 1 EECA consist of the cost of the hardware and software specified in § 113 subsection 5 EECA, the cost of maintenance thereof, the cost of transmission of messages to the surveillance devices and the cost of providing the information specified in § 112 subsections 1 and 3 EECA.

The cost of the hardware and software specified in § 113 subsection 5 EECA and the cost of maintaining them shall be compensated to the communications undertaking out of the state budget fees sector through the budget of the Ministry of Economic Affairs and Communications. Such fees shall be paid in the form of fixed payments to be made in yearly instalments during a period not exceeding ten years per one acquired object. The need to acquire or replace hardware or software,

the manner of acquisition and the costs of the acquisition and maintenance are subject to approval by the Ministry of Economic Affairs and Communications before the acquisition or replacement of the hardware or software. The fees are paid in accordance with the contract entered into between the Ministry of Economic Affairs and Communications and the communications undertaking.

The costs related to transmission of messages and provision of information shall be compensated to the communications undertaking out of the state budget through the budget of the ministry in the area of government to which the surveillance agency or security authority belongs. Such costs shall be compensated for in accordance with the contract entered into between the surveillance agency or security authority and the communications undertaking. The procedure for compensation for the costs provided for in § 114 subsections 3 and 4 EECA shall be established by the Government of the Republic.

6. Obligation to provide information to courts

§ 114^1 EECA provides that in order to establish the truth, a communications undertaking must provide the court, on the basis of single written requests thereof, with information at its disposal which is specified in § 111^1 subsections 2 and 3 EECA pursuant to the procedure and basis prescribed in the Code of Civil Procedure and within the term specified by the court. For the purposes of this section, a single request means a request for obtaining the information specified in § 111^1 clauses (2) and (3) EECA of concerning a particular telephone call, a particular electronic mail, a particular electronic commentary or another communication session related to the transmission of a single message.

7. Obligation to provide information to the Tax and Customs Board

§ 114^2 EECA provides that, following an order from the Tax and Customs Board to enable it to ascertain the facts relevant to tax proceedings, a communications undertaking is required to provide the data of the bill presented to the subscriber for the communications services, except for the information concerning the details of the communications services used.

8. Obligation to provide information to Estonian Information System Authority

§ 114^3 EECA provides that a communications undertaking is required, when requested by the Estonian Information System Authority, to submit the following information for the purpose of determining the devices which have caused or are compromised by a cyber incident:

1) the dates and times of beginning and end of the Internet session, based on a given time zone, together with the IP address allocated to the device by the provider of the data communication services;
2) the device's IP address protocol, the destination port of packets sent to the device and the source port of response packets.

9. Liability for the violation of EECA requirements

Chapter 14 EECA sets out liability for the violation of above-named requirements.

§ 154 EECA provides that failure to submit information specified in subsection 148 (2) is punishable by a fine of up to 100 fine units. The same act, if committed by a legal person, is punishable by a fine of up to 2000 euros.

§ 184^1 EECA provides that violation of the obligation to preserve the data specified in § 111^1, the log files specified in subsection 113 (5) or the application specified in subsection 113 (6) is punishable by a fine of up to 300 fine units. The same act, if committed by a legal person, is punishable by a fine of up to 3200 euros.

§ 185 EECA provides that violation of the obligation to provide information to a surveillance agency or security authority or to grant access to the communications network provided for in §§ 112 and 113 is punishable by a fine of up to 200 fine units. The same act, if committed by a legal person, is punishable by a fine of up to 2600 euros.

§ 186 EECA provides that violation of the obligation to maintain the confidentiality of information related to the conduct of surveillance activities and activities which restrict the right to inviolability of private life or the right to the confidentiality of messages provided for in subsection 113 (9) is punishable by a fine of up to 200 fine units. The same act, if committed by a legal person, is punishable by a fine of up to 2600 euros.

§ 187 EECA provides that violation of the obligation to maintain the confidentiality of information concerning the user which has become known in the process of provision of communications services or failure to give notice thereof is punishable by a fine of up to 200 fine units. The same act, if committed by a legal person, is punishable by a fine of up to 2000 euros.

B. Regulatory Framework for Surveillance Activities and Access to Data for Law Enforcement, Security, and Other Institutions

The right to submit the above-mentioned request is also provided and regulated by the:[12]

- Code of Criminal Procedure;
- Code of Misdemeanour Procedure;
- Police and Border Guard Act;
- Security Authorities Act;
- Taxation Act;
- Customs Act;
- Witness Protection Act;
- Estonian Defence Forces Organisation Act;
- Imprisonment Act;
- Aliens Act;
- Status of Members of the Riigikogu Act;
- Security Act;
- Securities Market Act;
- Strategic Goods Act;
- Weapons Act.

C. Powers in the Code of Criminal Procedure

The Estonian Code of Criminal Procedure (ECCP) provides the rules for pre-trial procedure and court procedure for criminal offences and the procedure for enforcement of the decisions made in criminal matters, as well as the basis of and procedure for conduct of surveillance activities. The taking of evidence by surveillance activities is regulated by chapter 3^1 of ECCP. Since 2013 inquiries to electronic communications undertakings are also possible, as § 90^1 ECCP provides that a body conducting proceedings may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in the public electronic communications network, except for the data relating to the fact of communication of messages.

With the permission of a Prosecutor's Office an investigative body may make enquiries in pre-trial procedure or with the permission of a court in court proceeding to electronic communications undertakings about the data listed in § 111^1 subsections 2 and 3 Electronic Communications Act (EECP) and not specified in the

[12] For the text and translation into English of the following legal Acts, please see annex.

first subsection of § 90[1] ECCP. The permission to make inquiries shall set out the dates of the period of time about which the requesting of data is permitted. The enquiries prescribed in this section may be made only if this is unavoidably necessary for the achievement of the objectives of criminal proceedings.

1. Surveillance activities

General conditions for conduct of surveillance activities are provided in § 126[1] ECCP. It provides that surveillance activities denote the processing of personal data for the performance of a duty provided by law with the objective of hiding the fact and content of data processing from the data subject.

Surveillance activities are permitted on the basis provided for in the ECCP if collection of data by other activities or taking of evidence by other procedural acts is impossible, is impossible in time or is especially complicated or if this may damage the interests of the criminal proceedings. Surveillance activities shall not endanger the life or health of persons, cause unjustified property and environment damage or unjustified infringement of other personality rights. Information obtained by surveillance activities can be used as evidence if application for and grant of authorisation for surveillance activities and the conduct of surveillance activities is in compliance with the requirements of law. Surveillance activities are conducted both directly through the institution specified in § 126[2] subsection 1 ECCP as well as the institutions, subordinate units, and employees administered by them and authorised to conduct surveillance activities, and through police agents, undercover agents, and persons recruited for secret cooperation.

A member of the *Riigikogu* or a rural municipality or city council, a judge, prosecutor, advocate, minister of religion or an official elected or appointed by the *Riigikogu* with his or her consent and a minor with the consent of his or her legal representative may be involved in the activities provided for in chapter 3[1] ECCP with the permission of a preliminary investigation judge only if they are parties to the proceeding or witnesses in the criminal matter concerned or a criminal offence is directed against them or a person close to them.

If the conduct of surveillance activities is requested by another investigative body, the surveillance agency which conducted the surveillance activities shall communicate the information obtained by the surveillance activities to the requesting investigative body together with the photographs, films, audio and video recordings and other data recordings made in the course of the surveillance activities. A surveillance agency also has the right, when conducting the surveillance activities, to process the data available from sources other than the surveillance activities.

2. Basis for conduct of surveillance activities

§ 126[2] subsection 1 ECCP provides that the Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Military Police and the Prisons Department of the Ministry of Justice and prisons (hereinafter *surveillance agency*) may conduct surveillance activities for the following:

1) a need to collect information about the preparation of a criminal offence for the purpose of detection and prevention thereof;
2) the execution of a ruling on declaring a person a fugitive;
3) a need to collect information in confiscation proceedings pursuant to the provisions of chapter 16[1] ECCP;
4) a need to collect information in a criminal proceeding about a criminal offence.

§ 126[2] subsection 2 ECCP provides that on the basis of the provisions of § 126[2] clauses (1) 1) and 4) ECCP surveillance activities may be conducted in the event of criminal offences specified in §§ 89–93[1], 95–97, 99, 100[1], 101–104, 106–108, 110–114, 116, 118 and 120, subsection 121 (2), §§ 133–137, 138[1] and 141–146, § 157[3], subsections 151 (2) and (4), subsection 161 (2), §§ 162, 163, 172–179, 183–185, 187–190, 199 and 200, subsections 201 (2) and (3), subsections 202 (2) and (3), §§ 204, 206–214, 216[1]–217, 217[2], 222, 227, 231–238, 241, 243, 244, 246, 250, 251, 255 and 256, clause 258 2), §§ 259, 259[1] and 263, subsections 266 (2) and (4), §§ 274, 290[1], 291, 291[1], 294, 296, 298–299, 300, 300[1], 302, 303, 310–313 and 315–316[1], subsection 321 (2), §§ 326–328, 331, 331[3], 333–334, 335, 336, 340 and 347, 356 subsections (1) and (3), subsections 357 (1) and (3), subsections 361 (1) and (3), 364 subsections (2) and (3), §§ 375–376[2], 384, 389[1], 391, 393 and 394, 398 subsections (2) and (4), 398[1] subsections (2) and (4), §§ 400, 402[3], 402[4], 403–407, 414–416, 418, 418[1], 421[1], 421[2], 434, 435 and 437–439, 440 subsections (3) and §§ 446 and 449 of the national Penal Code.

On the basis of ECCP, surveillance activities may be conducted in respect of the following persons:

1) on the basis specified in § 126[2] clause (1) 1) ECCP in respect of the person in the case of whom there are serious reasons to believe that he or she commits the criminal offence specified in § 126[2] subsection 2 ECCP;
2) on the basis specified in § 126[2] clause (1) 2) ECCP in respect of the person who is declared to be a fugitive;
3) on the basis specified in § 126[2] clause (1) 3) ECCP in respect of the person who owns or possesses the assets which are the object of confiscation proceedings;
4) on the basis specified in § 126[2] clause (1) 4) ECCP in respect of the person who is a suspect in a criminal proceeding or with respect to whom there is justified reason to believe that he or she has committed or commits the specified criminal offence.

The surveillance activities conducted on the basis provided for in § 126^2 clauses (1) 2)–4) ECCP may also be conducted in respect of the person with regard to whom there is good reason to believe that he or she interacts with the person specified in § 126^2 clauses (3) 2)–4) ECCP, communicates information to them, provides assistance to them or allows them to use their means of communication, and if the conduct of surveillance activities in respect of such person may provide the data required for the achievement of the objective of the surveillance activities.

A surveillance agency may conduct surveillance activities on the basis specified in § 126^2 subsection 1 ECCP if this is related to a criminal offence which is in the investigative jurisdiction of such surveillance agency. A surveillance agency may conduct surveillance activities at the request of another surveillance agency within the limits of its competence under the conditions and pursuant to the procedure provided for in ECCP. The Police and Border Guard Board and the Security Police may also conduct surveillance activities at the request of other investigative bodies. The Prisons Department of the Ministry of Justice and prisons may also conduct surveillance activities in a custodial institution at the request of other investigative bodies.

Where the basis for surveillance activities ceases to exist, the surveillance activities shall be immediately terminated.

Surveillance activities may be conducted outside the ECCP only on the basis provided for in the Estonian Defence Forces Organisation Act, Taxation Act, Police and Border Guard Act, Weapons Act, Strategic Goods Act, Customs Act, Witness Protection Act, Security Act, Imprisonment Act, Aliens Act, and Obligation to Leave and Prohibition on Entry Act. The provisions of this chapter of ECCP apply to the conduct of surveillance activities, processing of information collected by surveillance activities, giving notification of surveillance activities and submission of information collected for examination with the specifications provided for in the Acts specified above.

3. List of surveillance activities

§ 126^3 ECCP provides that on the basis specified in § 126^2 subsection 1 ECCP, a surveillance agency may covertly watch a person, thing or area, covertly take comparative samples and perform initial examinations, covertly examine a thing and covertly replace it. The Police and Border Guard Board and the Security Police Board may conduct the following surveillance activities on the basis specified in § 126^2 clause (1) 1) ECCP upon collection of information concerning the preparation for the criminal offence specified in §§ 244 and 246, 266 clause (2) 3) and §§ 255 and 256 Penal Code and on the basis specified in clauses 3) and 4):

1) to covertly examine a postal item;

2) to covertly observe or wire-tap information;

3) to use a police agent.

The Prisons Department of the Ministry of Justice and prisons may conduct the following surveillance activities specified in § 126^2 clauses (1) 1) and 4) ECCP:

1) to covertly examine a postal item;

2) to covertly observe or wire-tap information.

Covert entry into a building, premises, vehicle, enclosed area or computer system is permitted upon conduct of the surveillance activities specified in subsection (1) and § 126^3 clauses (2) 2) and 3) ECCP if this is unavoidably necessary for the achievement of the objectives of the surveillance activities. For the purposes of ECCP, entry into the possessions of other persons is deemed to be covert if the fact of entry is covert for the possessor or if a misconception of existing facts is knowingly caused by fraud upon entry and the possessor, with knowledge of the actual circumstances, would not have given possession for entry.

4. Grant of permission for surveillance activities

§ 126^4 ECCP provides that surveillance activities may be conducted with a written permission of a Prosecutor's Office or a preliminary investigation judge. The preliminary investigation judge shall decide the grant of permission by a ruling on the basis of a reasoned application of the Prosecutor's Office. The preliminary investigation judge shall immediately review a reasoned request submitted by a Prosecutor's Office and grant or refuse to grant permission for the conduct of the surveillance activities by a ruling.

In cases of urgency, surveillance activities requiring the permission of a Prosecutor's Office may be conducted with the permission of the Prosecutor's Office issued in a format which can be reproduced in writing. A written permission shall be formalised within 24 hours of the commencement of surveillance activities. In the case of immediate danger to the life, physical integrity or physical freedom of a person or to proprietary benefits of high value and requesting a permission or execution thereof on time is impossible, surveillance activities requiring the permission of a court may be conducted, in cases of urgency, with the permission of the court issued in a format which can be reproduced in writing. A written application and permission shall be formalised within 24 hours of the commencement of surveillance activities.

A permission issued in cases of urgency in a format which can be reproduced in writing shall contain the following information:

1) the issue of the permission;

2) the date and time of issue of the permission;

3) surveillance activities for which the permission is issued;

4) if known, the name of the person with regard to whom the surveillance activities are conducted;

5) the term of the permission for surveillance activities.

If covert entry into a building, premises, vehicle, enclosed area or computer system is necessary for conduct of surveillance activities or in order to install or remove technical appliances necessary for surveillance, a Prosecutor's Office shall apply for a separate permission of a preliminary investigation judge for such purpose.

The duration of surveillance activities conducted with respect to a specific person on the basis provided for in § 126^2 clauses (1) 1), 3) and 4) ECCP in the same proceedings must not exceed one year. In exceptional cases, the Prosecutor General may authorise or apply to a court for authorisation to conduct surveillance activities for more than one year.

5. Covert surveillance, covert collection of comparative samples and conduct of initial examinations, covert examination and replacement of things

§ 126^5 ECCP provides that a Prosecutor's Office shall issue permission for covert surveillance of persons, things or areas, covert collection of comparative samples and conduct of initial examinations and covert examination or replacement of things for up to two months. The Prosecutor's Office may extend the term of the permission for up to two months at a time. In the course of the surveillance activities specified in this section, the information collected shall be, if necessary, video recorded, photographed or copied or recorded in another way.

6. Wire-tapping or covert observation of information

§ 126^7 ECCP provides that information obtained by wire-tapping or covert observation of messages or other information transmitted by the public electronic communications network or communicated by any other means shall be recorded.

Information communicated by a person specified in § 72 ECCP or information communicated to such person by another person who is subject to wire-tapping or covert observation shall not be used as evidence if such information contains facts which have become known to the person in his or her professional activities, unless:

1) the person specified in § 72 ECCP has already given testimony with regard to the same facts or if the facts have been disclosed in any other manner;
2) a permission has been granted with respect to such person for wire-tapping or covert observation; or
3) it is evident on the basis of wire-tapping or covert observation of another person that the specified person commits or has committed a criminal offence.

A preliminary investigation judge grants permission for the surveillance activities specified in § 126^7 ECCP for up to two months. After expiry of the specified term, the preliminary investigation judge may extend this term by up to two months.

7. Documentation of surveillance activities

§ 126[10] ECCP provides that on the basis of the information collected by surveillance activities, an official of the body that conducted surveillance activities or applied for surveillance activities shall prepare a report on surveillance activities which shall set out:

1) the name of the body which conducted the surveillance activities;
2) the time and place of conducting the surveillance activities;
3) the name of the person with regard to whom the surveillance activities were conducted;
4) the date of issue of a permission of a court or a permission of a Prosecutor's Office which is the basis for surveillance activities;
5) the date of submission of an application of a Prosecutor's Office if the surveillance activities are based on a permission of a court;
6) information collected by surveillance activities which is necessary to achieve the objectives of surveillance activities or to adjudicate a criminal matter.

The photographs, films, audio and video recordings, and other data recordings made in the course of surveillance activities shall be appended to a report, if necessary. If necessary, the surveillance agency that conducted surveillance activities shall record the information collected by surveillance activities in a summary of surveillance activities. The summary of surveillance activities and the photographs, films, audio and video recordings, and other data recordings made in the course of surveillance activities shall be appended to a surveillance file.

a) Duty to keep surveillance files

§ 126[11] ECCP provides that the information collected by surveillance activities, data recordings made in the course of surveillance activities, data obtained in the manner specified in § 126[1] subsection 8 ECCP and data required for comprehension of the integrity of the information collected by surveillance activities concerning an undercover agent and simulated person, structural unit, body, and branch of a foreign company shall be stored in a surveillance file. The procedure for keeping and storage of surveillance files shall be established by a regulation of the Government of the Republic on the proposal of the minister responsible for the area.

b) Storage, use, and destruction of surveillance files and data recordings collected by surveillance activities

§ 126[12] ECCP provides that the photographs, films, audio and video recordings, and other data recordings or any part thereof necessary for the adjudication of a criminal matter and made in the course of surveillance activities shall be stored in the criminal file or together with the criminal matter. The rest of the materials on

surveillance activities shall be stored at surveillance agencies pursuant to the procedure specified in § 126[11] subsection 2 ECCP.

Surveillance files shall be stored as follows:

1) surveillance files kept on criminal offences under preparation, files on searching persons, and confiscation files – until the redundancy of information contained therein, but for not longer than 50 years;
2) files on criminal offences – until the deletion of data concerning punishment from the punishment register or expiry of the limitation period for the criminal offence.

The information collected by surveillance activities may be used in other surveillance activities, other criminal proceedings, security checks, in deciding, in the cases provided by law, upon hiring persons and grant of permissions or licences to verify the conformity of the person to the requirements provided by law. The information collected by surveillance activities may be stored for study and research purposes. Personal data and, if necessary, the information collected shall be completely altered in order to prevent disclosure of persons who have been engaged in surveillance activities or recruited for them.

If preservation of a data recording made in the course of surveillance activities and added to a criminal file is not necessary, the person subject to the surveillance activities whose fundamental rights were violated by such surveillance activities may request destruction of the data recording after the entry into force of the court judgment. The data recording specified in § 126[12] subsection 5 ECCP shall be destroyed by a court. A report shall be prepared on the destruction of a data recording and included in the criminal file.

If the materials on surveillance activities are stored in a criminal file, the information concerning the persons accused in criminal proceedings whose private or family life was significantly violated by the surveillance activities and whose rights or freedoms may be significantly damaged by disclosure shall be removed from or covered up in the criminal file upon disclosure thereof pursuant to the Public Information Act. Files containing a state secret or classified information of a foreign state shall be stored and destroyed pursuant to the State Secrets and Classified Information of Foreign States Act.

Surveillance files subject to destruction and data recordings collected shall be destroyed by a committee formed by the head of a surveillance agency in the presence of a prosecutor. The committee shall prepare a report concerning the destruction of a file and data recording collected which shall set out the number of the file or information concerning the destructed data recording and the reason for the destruction thereof.

8. Duty to notify, oversight and remedies

a) Duty of notification

§ 126[13] ECCP provides that upon expiry of the term of permission for the conduct of surveillance activities and, when several surveillance activities are conducted that coincide at least partly in time, upon expiry of the term of the last permission, the surveillance agency shall immediately notify the person with respect to whom the surveillance activities were conducted and the person whose private or family life was significantly violated by the surveillance activities and who was identified in the course of the proceedings. The person shall be notified of the time and type of surveillance activities conducted against them.

With the permission of a prosecutor, a surveillance agency need not give notification of conduct of surveillance activities if this may:

1) significantly damage the criminal proceedings;
2) significantly damage the rights and freedoms of another person which are guaranteed by law or endanger another person;
3) endanger the confidentiality of the methods and tactics of a surveillance agency, the equipment or police agent used in conducting surveillance activities, of an undercover agent or person who has been recruited for secret cooperation.

With the permission of a Prosecutor's Office, a person need not be given notification of surveillance activities until the basis specified in § 126[13] subsection 2 ECCP ceases to exist. The Prosecutor's Office shall verify the basis for non-notification in a criminal matter upon completion of pre-trial proceedings but not later than one year after the expiry of the term of the permission for surveillance activities.

If the basis for non-notification of surveillance activities has not ceased to exist upon expiry of one year as of the expiry of the term of the permission for surveillance activities, a Prosecutor's Office applies, at the latest 15 days prior to the expiry of the specified term, for the permission of a preliminary investigation judge for extension of the non-notification term. The preliminary investigation judge grants permission by a ruling for non-notification of the person or refuses to grant such permission. Upon non-notification of a person, the ruling shall set out whether the non-notification is granted for an unspecified or specified term. In the case of non-notification during a specified term, the term during which a person is not notified shall be set out.

If the basis specified in § 126[13] subsection 2 ECCP has not ceased to exist upon expiry of the term of the permission granted for non-notification by a preliminary investigation judge specified in § 126[13] subsection 4 ECCP, a Prosecutor's Office applies, at the latest 15 days prior to expiry of such term, for permission from a preliminary investigation judge for extension of the non-notification term. The pre-

liminary investigation judge grants permission by a ruling pursuant to the provisions of § 126[13] subsection 4 ECCP.

A person shall be immediately notified of surveillance activities upon expiry of the permission for non-notification or refusal to grant permission for the extension thereof. When a person is notified of surveillance activities conducted against them, the procedure for appeal shall be explained to them.

b) Submission of information collected by surveillance activities for examination

§ 126[14] ECCP provides that the person who has been notified pursuant to § 126[13] ECCP shall be permitted at his or her request to examine the data collected against them and the photographs, films, audio and video recordings, and other data recordings made in the course of the surveillance activities. With the permission of a Prosecutor's Office, the following information need not be submitted until the corresponding basis ceases to exist:

1) information concerning the family or private life of other persons;
2) information the submission of which may damage the rights and freedoms of another person which are guaranteed by law;
3) information which contains state secrets, classified information of foreign states or secrets of another person that are protected by law;
4) information the submission of which may endanger the life, health, honour, good name, and property of an employee of a surveillance agency, police agent, undercover agent, person who has been recruited for secret cooperation or another person who has been engaged in surveillance activities or of persons connected with them;
5) information the submission of which may endanger the right of a police agent, undercover agent, and person who has been recruited for secret cooperation to maintain the confidentiality of cooperation;
6) the submission of which may result in communication of information concerning the methods, tactics of a surveillance agency, and the equipment used in conduct of surveillance activities;
7) information which cannot be separated or disclosed without information specified in § 126[14] subsection 1 clauses 1)–6) ECCP becoming evident.

Upon submission of or refusal to submit information collected by surveillance activities for examination to a person, the procedure for appeal shall be explained to them. The procedure for notification of surveillance activities and submission of surveillance files shall be established by a regulation of the Government of the Republic on the proposal of the minister responsible for the area.

c) Oversight of surveillance activities

§ 126[15] ECCP provides that a Prosecutor's Office shall exercise supervision over the compliance of surveillance activities with the permission provided for in § 126[4] ECCP.

The committee of *Riigikogu* specified in § 36 Security Authorities Act shall exercise supervision over the activities of surveillance agencies. A surveillance agency shall submit a written report to the committee through the appropriate ministry at least once every three months.

The Ministry of Justice shall publish on its website once a year a report on the basis of the information obtained from surveillance agencies, Prosecutor's Offices and courts, which contains the following information concerning the previous year:

1) number and type of opened surveillance files;
2) number of permissions for surveillance activities by types of surveillance activities;
3) number of persons notified of conduct of surveillance activities and number of persons in the case of whom notification was postponed pursuant to § 126[13] subsection 4 ECCP for more than one year.

d) Filing of appeals in connection with surveillance activities

§ 126[16] ECCP provides that an appeal may be filed pursuant to the procedure provided for in chapter 15 of the ECCP against the court ruling that grants permission for surveillance activities on the basis specified in the Code. An appeal may be filed pursuant to the procedure provided for in ECCP Division 5 chapter 8 against the course of surveillance activities conducted on the basis specified in the Code, non-notification thereof and refusal to submit information collected thereby.

9. Surveillance activities information system

§ 126[17] ECCP provides that the surveillance activities information system (hereinafter *information system*) is a database belonging to the State Information Systems maintained for processing of the surveillance activities information provided for in the ECCP, the objective of which is to:

1) provide an overview of surveillance activities conducted by surveillance agencies;
2) provide an overview of requests of surveillance agencies and Prosecutor's Offices for conduct of surveillance activities;
3) provide an overview of permissions issued by Prosecutor's Offices and courts for conduct of surveillance activities;

4) provide an overview of notification of surveillance activities and submission of information collected by surveillance activities;
5) reflect information concerning the surveillance activities conducted;
6) enable the organisation of the activities of surveillance agencies, Prosecutor's Offices and courts;
7) collect statistics on surveillance activities which are necessary for the making of decisions concerning criminal policy;
8) enable electronic forwarding of data and documents.

The information system shall be established and the statutes thereof shall be approved by the Government of the Republic. The chief processor of the information system is the Ministry of Justice. The minister responsible for the area may organise the activities of the information system by a regulation.

D. Powers under Code of Misdemeanour Procedure and Police and Border Guard Act

1. The Code of Misdemeanour Procedure

The Code of Misdemeanour Procedure (CMP),[13] passed on 22 May 2002 which entered into force on 1 September 2002, provides for the extra-judicial and court procedure for misdemeanours and for execution of the punishments imposed for misdemeanours. Unless otherwise provided for in the CMP, the provisions concerning criminal procedure apply to misdemeanour proceedings, taking into account the specifications arising from misdemeanour proceedings.

2. The Police and Border Guard Act

The Police and Border Guard Act (PBGA),[14] passed on 6 May 2009 and entered into force on 1 January 2010 (and also partially on 1 January 2012), provides for the functions, rights, and organisation of the police and the legal basis of the police service. The functions and activity of the police in offence proceedings have been provided for in the ECCP and in the CMP. The Law Enforcement Act shall apply to the functions and activity of the police upon protection of the public order, taking into account the specifications arising from this Act.

---

[13] For the text and translation into English of the Act, please see annex.
[14] For the text and translation into English of the Act, please see annex.

3. Request to electronic communications undertakings to submit information

§ 312 CMP provides that the Data Protection Inspectorate, the Financial Supervision Authority, the Estonian Internal Security Service, the Environmental Inspectorate, the Tax and Customs Board, and the Police and Border Guard Board may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in the public electronic communications network, except for the data relating to the fact of transmission of messages. With the permission of a court, the institution specified in § 31^2 subsection 1 CMP may make a single enquiry to electronic communications undertakings about the data listed in subsections 111^1 (2) and (3) ECA and not specified in § 31^2 subsection 1 CMP. For the purposes of this section, a single request is a request for obtaining the information specified in subsections 111^1 (2) and (3) concerning a particular telephone call, electronic mail, electronic commentary or another communication session related to the transmission of a single message. The enquiries specified in this section may be made only if this is unavoidably necessary for the achievement of the objectives of misdemeanour proceedings.

4. Making an enquiry to a communications undertaking

§ 7^{49} CMP provides that the police may make an enquiry to an electronic communications undertaking on the basis specified in § 126^2 clause (1) 1) and 2) ECCP and with respect to persons specified in § 126^2 clause (3) 1) and 2) ECCP in order to obtain the following information:

1) information necessary to identify an end user related to identification characteristics used in an electronic communications network, except for information related to the fact of message forwarding;
2) to an electronic communications undertaking, information specified in § 111^1 subsections (2) and (3) ECA and not specified in subsection (1) of this section.

Making an enquiry specified in § 7^{49} clause (1) 2) CMP shall be authorised by the Prosecutor's Office. The authorisation for making an enquiry shall set out the period of validity for the permission to require information.

5. Collection of information for deciding on the access of a person to surveillance information and on suitability of a person for police service

§ 7^{50} CMP provides that the police may, with the written consent of a person, collect personal data concerning the person by surveillance activity specified in subsection 126^3 (1) ECCP and by an enquiry to an electronic communications undertaking with respect to information provided for in subsections 111^1 (2) and (3) ECA if it is necessary in order to decide on the person's access to surveillance information or to verify information presented in the personal data form for deciding

his or her suitability for the police service. A person shall be notified of surveillance activity referred to in § 7^{50} subsection 1 CMP conducted with respect to the person after a decision has been made and he or she shall be shown, at his or her request, the information collected by the surveillance activity. Information collected by an enquiry referred to in § 7^{50} subsection 1 CMP shall be shown to the person at his or her request.

6. Collection of information for verifying the suitability of a person for recruitment for secret cooperation and for verifying credibility of information

§ 7^{52} CMP provides that the police may, with the written consent of a person, collect personal data by surveillance activity specified in § 126^3 clause (1) and in § 126^3 clause (2) 2) ECCP and by an enquiry to an electronic communications undertaking with respect to information provided for in § 111^1 (2) and (3) ECA if it is necessary in order to decide on the person's suitability for secret cooperation or for verifying the credibility of information. The surveillance activity specified in § 126^3 clause (2) 2) ECCP is allowed when all other verification means have been exhausted and there is reasonable doubt as to the reliability of the person which may jeopardise the purpose of the secret cooperation, or there is reasonable doubt as to the credibility of information and this may significantly infringe the fundamental rights of persons or influence the course of the criminal proceedings.

An authorisation for performing the surveillance activity specified in § 126^3 clause (1) ECCP and for making an enquiry for obtaining information provided for in § 111^1 clauses (2) and (3) ECA shall be granted by the Director General of the Police and Border Guard Board or an official authorised thereby. An authorisation for performing the surveillance activities specified in § 126^3 clause (2) 2) ECCP shall be granted by the county court on the basis of a justified written application of the Director General of the Police and Border Guard Board.

E. Powers under the Security Authorities Act

1. The Security Authorities Act

The Security Authorities Act (SAA),[15] passed on 20 December 2000 and entered into force on 1 March 2001, provides for the functions and competence of security authorities in ensuring national security and constitutional order, and the procedure for the exercise of supervision over the activities of security authorities. The provisions of the Administrative Procedure Act apply to administrative proceedings prescribed in the SAA, taking account of the specifications provided for in this Act.

[15] For the text and translation into English of the Act, please see annex.

The security authorities are the Estonian Internal Security Service and the Estonian Foreign Intelligence Service.

2. Objective of the security authorities

§ 2 SAA provides that the objective of the activity of the security authorities is to ensure national security by the continuance of constitutional order through the application of non-military means of prevention, and to collect and process information necessary for formulating the security policy and for national defence. Achievement of the objectives specified in § 2 subsection 1 SAA shall take place through the Defence Forces pursuant to the procedure provided for in this Act unless otherwise provided by the Estonian Defence Forces Organisation Act.

3. Co-operation between security authorities

§ 11 SAA provides that security authorities shall co-operate with each other through mutual assistance and exchange of information. Exchange of information between the security authorities shall take place on the basis of the plan regarding the obtaining and analysis of state security information.

4. Principles of activity of security authorities

§ 3 SAA provides that security authorities collect and process information, including personal data, insofar as this is necessary for performing their functions. A security authority shall only use measures necessary for performing its functions. If there are several possible measures, the security authority shall use the measure which is least infringing of the fundamental rights of the person in connection with the performance of a function of the security authority. A measure, which does not restrict the fundamental rights of an individual excessively compared to the objective pursued by the security authority, may be used.

5. Manner of collection of information

§ 24 SAA provides that information, including personal data, shall be collected, for the performance of the functions of a security authority, directly by the security authority or the authority authorised for such purpose or by a person recruited for cooperation. Collection of information shall not damage the life, health or property of persons or the environment.

6. Restrictions on personal rights and safeguards

a) Restrictions on the right to confidentiality of messages

§ 25 SAA provides that in the cases provided for in this section, a security authority is permitted to restrict a person's right to the confidentiality of messages sent or received by them by post, telegraph, telephone or other commonly used means. A security authority may, within the limits of its competence, restrict a person's right to the confidentiality of messages in order to combat a criminal offence if there is sufficient information to indicate that a criminal offence is being prepared or committed.

A person's right to the confidentiality of messages is restricted by:

1) examination of a postal item;
2) wire-tapping, observing or recording a message or other information transmitted over an electronic communications network;
3) wire-tapping, observing or recording information communicated by any other means.

b) Restrictions on the right to inviolability of home, and family or private life

§ 26 SAA provides that security authorities may restrict a person's right to the inviolability of home, and family or private life in the cases provided for in this section. An official of a security authority may, within his or her competence and in order to combat a criminal offence, enter or search a person's premises, building, enclosed area, vehicle or computer system without the consent of the person on the order of the head of the security authority in order to ensure national security or if there is sufficient information to indicate that a criminal offence is being prepared or committed and if collection of information is necessary for combating the criminal offence.

A person's right to the inviolability of home, and family or private life is restricted by:

1) collection of personal data;
2) covert surveillance;
3) covert establishment of identity;
4) collection of information on the fact, duration, manner, and form of transmission of messages over an electronic communications network, and on the personal data and location of the sender or receiver of such messages;
5) covert entry in the person's premises, building, enclosed area, vehicle or computer system for the purposes of covert collection or recording of information or installation and removal of technical aids necessary for such purposes.

6) covert examination of an item and, if necessary, covert alteration of the item, damage to the item or replacement of the item.

On the basis of a written agreement entered into with a security authority and within the competence of the security authority, a person recruited for secret co-operation may also restrict a person's right to the inviolability of home, and family or private life pursuant to the procedure provided for in § 27 SAA.

c) Procedure for restriction of the right to confidentiality of messages and the right to inviolability of home, and family or private life

§ 27 SAA provides that in the case of a need to restrict a person's right to the confidentiality of messages or to the inviolability of home, and family or private life in the manner specified in § 26 clause (3) 5) SAA, the head of a security authority shall submit to the chairman of an administrative court or an administrative judge appointed by the chairman a reasoned written application for the corresponding permission. The application shall set out the manner of restriction of the corresponding right.

Grant, extension, and revocation of a permission and declaration as justified of restriction of a person's right to the confidentiality of messages or to the inviolability of home, and family or private life in the manner specified in § 26 clause (3) 5) SAA shall be decided without delay and without holding a court session, pursuant to the provisions of the Code of Administrative Court Procedure concerning granting permission for administrative measures. Permission may be granted for a period of up to two months or extended for the same period each time.

In emergencies if there is a threat to the national security or if there is sufficient information to indicate that a criminal offence is being prepared or committed and the act specified in § 27 subsection 1 SAA is necessary to combat a criminal offence and it is impossible to apply for the permission specified in § 27 subsection 2 SAA, the act may be performed with the permission of the administrative court, which is issued in a manner which can be reproduced. The head of the security authority shall submit a reasoned application which can be reproduced as a basis for the permission to the chairman of an administrative court or an administrative judge appointed by the chairman at the first opportunity but no later than on the day following the commencing of the act. The application sets out the manner and duration of the restriction of the specified right. The chairman of an administrative court or an administrative judge appointed by the chairman shall decide on the continuation of the act with the permission specified in § 27 subsection 2 SAA.

The permission which is issued in an emergency in a manner which can be reproduced shall include the following data:

1) the name of the person who issued the permission;

2) the date and time of issue of the permission;

3) the act for the performance of which the permission is issued;

4) the name of a person with regard to whom the act is performed if it is known;

5) the term of the permission.

Restriction of a person's right to the inviolability of home, and family or private life shall be decided, by an order, by the head of a security authority or an official authorised by them. An order shall be valid for the term indicated therein but for no longer than two months. The acts specified in § 25 clause (3) 2) and in § 26 clause (3) 4) SAA shall be performed in accordance with the relevant provisions of the ECA.

7. Methods and means of covert collection of information

§ 28 SAA provides that the methods and means to be used by a security authority in covert collection of information shall be established by the relevant minister by a regulation. The regulation shall be submitted to the Security Authorities Surveillance Committee of the *Riigikogu* for information purposes.

8. Notifying a person of means used

§ 29 SAA provides that security authority shall notify a person whose fundamental rights are restricted in the manner provided for in §§ 25 or 26 SAA immediately of the measures used and the circumstances relating to the restriction of fundamental rights if this does not endanger the aim of the restriction, or after such danger ceases to exist.

9. Storage of information

§ 30 SAA provides that information collected in the manner provided for in §§ 25 or 26 of this Act shall be stored in information files. A separate information file shall be opened for each individual case. The procedure for keeping and storing files shall be established by a regulation of the minister responsible for the field governed by the Ministry of the Interior or the Ministry of Defence.

10. Communication of information to security authorities

§ 31 SAA provides that in order to obtain data necessary for the performance of the functions of a security authority, the authority may request such data from a state or local government authority or a legal person in public law if such data cannot be obtained from a publicly available source or it would result in disproportionate costs or more onerous measures for the person whose personal data is communicated. A security authority has the right to obtain information necessary for the performance of its functions from a natural person or a legal person in private law.

Disclosure of personal data is not mandatory if the security authority fails to justify the need to obtain the data or if disclosure of such data is not permitted.

11. Access to databases

§ 31[1] SAA provides that for the performance of their functions imposed by law, security authorities have access, free of charge, to information held in databases established on the basis of the Public Information Act.[16]

12. Communication of information by security authorities

§ 32 SAA provides that information which is received in the performance of the functions of a security authority must be communicated to another state authority if it is necessary for the performance of the functions imposed on the state authority and it does not harm the performance of the functions of the security authority. Information which is received in the performance of the functions of a security authority must be communicated to another state authority and to a natural or legal person if it is necessary for combating a crime of terrorism or if it is related to a threat of commission of a crime of terrorism and it does not harm the performance of the functions of the security authority. Information which is received in the performance of the functions of a security authority may be communicated to a company with state participation if it is necessary for the performance of its functions and it does not harm the performance of the functions of the security authority. For the purposes specified in § 32 subsections 1–3 SAA, a security authority, a state authority and a person to whom information has been communicated may process information containing personal data without the consent of the data subject.

13. Organization of protection of communications

§ 23[1] SAA provides that the requirements for special communications services shall be established by a regulation of the minister responsible for the field. The regulation shall be submitted to the Security Authorities Surveillance Committee of the *Riigikogu* for information purposes.

14. Use of legal persons in private law

§ 23[1] SAA provides that security authority may use a legal person in private law for the performance or ensuring the performance of its functions on the basis of the resolution of the head of the security authority, using shadow information or covert measures pursuant to the procedure specified in § 23 SAA. Every six months the

---

[16] For the text and translation into English of the Act, please see annex.

head of the security authority shall submit to the relevant minister information concerning the activities of a legal person in private law specified in subsection (1) of this section.

F. Powers Under Other Legislation

1. The Taxation Act

The Taxation Act,[17] passed on 20 February 2002 and entered into force on 1 July 2002 pursuant to § 170, specifies the rights, obligations and liability of tax authorities and taxable persons, the procedure for tax proceedings, and the procedure for the resolution of tax disputes. The Law Enforcement Act shall be applied to state supervision exercised on the basis of this Taxation Act with the specifications provided in this Act. The Taxation Act § 81^1 provides that the Tax and Customs Board may make an enquiry to an electronic communications undertaking on the basis specified in § 126^2 clauses (1) 1) and 2) ECCP and with regard to the persons specified in § 126^2 clauses (3) 1) and 2) ECCP to get the following information:

1) the information needed to establish the end-user connected to the identifier of the user used in the electronic communication network, except the information concerning the fact of transmission of messages;
2) the information to the electronic communications undertaking specified in subsections 111^1 (2) and (3) ECA which are not mentioned in clause 1) of this subsection.

The authorisation for making the enquiry specified in § 81^1 clause (1) 2) Taxation Act shall be granted by the Prosecutor's Office. The authorisation for making an inquiry shall set out the interval for which the request for information is allowed with a timeframe.

Taxation Act § 81^2 provides that The Tax and Customs Board may, with the written consent of the person, collect personal information with regard thereto by means of surveillance proceedings specified in § 126^3 clause (1) ECCP and by means of the enquiry to the communications undertaking with regard to the information specified in § 111^1 clauses (2) and (3) ECA if this is needed for making a decision with regard to a person to allow access to surveillance information concerning them or for employment of a person in the Tax and Customs Board. After a decision is made a person shall be notified of the conduct of proceedings specified in § 81^2 subsection 1 Taxation Act against them and they shall be familiarised with the data collected by means of the proceeding at their request.

---

[17] For the text and translation into English of the Act, please see annex.

§ 81[3] Taxation Act provides that in order to ensure the conduct of covert investigation the Tax and Customs Board is entitled to involve persons in secret cooperation and use undercover agents to ensure the conduct of surveillance activities and collection of information, as well as use covert measures under the conditions provided in the Police and Border Guard Act. The head of the Tax and Customs Board or a person appointed by them shall give written permission for the involvement of a person. The head of the Tax and Customs Board shall give written permission for involvement of an undercover agent. The document necessary for performance of covert measures shall be issued and the necessary amendment in the database or register shall be made by an administrative body or legal person whose competence involves the issue of such document or making amendments in the database or register on the basis of the reasoned request of the head of the Tax and Customs Board or an official authorised by them.

2. The Customs Act

The Customs Act,[18] passed on 31 May 2017 and entered into force on 1 January 2018, provides for supplementing requirements for the conveyance of goods from outside the customs territory of the European Union (EU) to Estonia and from Estonia to outside of the customs territory of the EU insofar as not governed by EU customs legislation, and measures of customs supervision and liability for violation of the customs legislation.

§ 10 Customs Act provides that Tax and Customs Board may collect personal information concerning a person with the written consent thereof by means of surveillance activities specified in § 126[3] (1) ECCP and by means of an enquiry to an electronic communications undertaking with regard to the information set out in § 111[1] (2) and (3) ECA if it is necessary in order to decide on the person's access to surveillance information or to employ the person in the service of the Tax and Customs Board. After a decision is made, the person shall be informed of the activities or enquiry specified in § 10 subsection 1 Customs Act conducted with respect to the person and the information collected by the activities shall be introduced to them at their request. § 11 Customs Act provides that for performing surveillance activities, ensuring the performance of surveillance activities or collecting information, the Tax and Customs Board has the right to recruit persons for secret cooperation and use undercover agents as well as use covert measures on the conditions provided by the Police and Border Guard Act.

Written authorisation for recruiting a person shall be granted by the Director General of the Tax and Customs Board or an official appointed thereby. Written authorisation for using an undercover agent shall be granted by the Director General of the Tax and Customs Board. The document necessary for taking covert

[18] For the text and translation into English of the Act, please see annex.

measures shall be issued and the necessary changes in the relevant database or register shall be made, on the basis of a reasoned request of the Director General of the Tax and Customs Board or an official authorised thereby, by an administrative authority or a legal person who is competent to issue such a document or make changes in the database or register.

§ 12 Customs Act provides that Tax and Customs Board may make an enquiry to an electronic communications undertaking on the basis specified in § 126^2 (1) 1) and 2) ECCP and with respect to the persons specified in § 126^2 (3) 1) and 2) ECCP in order to obtain the following information:

1) information necessary to identify the end user related to the identifiers used in the electronic communications network, except for information related to the fact of transmission of messages;
2) information specified in § 111^1 (2) and (3) ECA given to the electronic communications undertaking and not specified in § 12 Customs Act provides subsection 1.

Making an enquiry concerning information specified in § 12 clause (1) 2) Customs Act shall be authorised by the Prosecutor's Office. The authorisation for making an enquiry shall set out the timeframe in which it is allowed to require information.

3. The Witness Protection Act

The Witness Protection Act (WPA),[19] passed on 15 June 2005 and entered into force on 21 July 2005, provides for:

1) the procedure for witness protection, the legal basis for witness protection authorities and their activities and for the application of protection measures;
2) the procedure for the performance of the international obligations of the Republic of Estonia related to protection of participants in criminal proceedings.

The provisions of the Administrative Procedure Act apply to administrative proceedings prescribed in the WPA, taking account of the specifications provided for in this Act.

In applying the measures of witness protection, the severity of a criminal offence under investigation, the significance of the evidence given by the person in the criminal case and the extent of the risk to the protected person are taken into account. Witness protection measures can be applied to a person only with the consent of the person or his or her legal representative or guardianship authority. Witness protection is carried out by the Police and Border Guard Board. Other state and local government bodies and authorities and legal persons in public law are

[19] For the text and translation into English of the Act, please see annex.

required to assist in witness protection within the limits of their competence. Supervision over witness protection activities shall be exercised by the Office of the Prosecutor General. The Police and Border Guard Board organises international co-operation in witness protection with competent foreign authorities and international organisations pursuant to international agreements.

§ 18^1 WPA provides that upon processing witness protection applications and application of protective measures, the witness protection authority is entitled to conduct the surveillance activities specified in subsection (1) and § 126^3 clauses (2) 1) and 2) ECCP, and the enquiries for obtaining the information prescribed in § 111^1 clauses (2) and (3) ECA. Permission for the surveillance activities specified in § 126^3 clause (1) ECCP and an inquiry for the data prescribed in § 111^1 ECA is granted by the head of the witness protection authority or an official authorised by them. Permission for surveillance activities specified in § 126^3 clauses (2) 1) and 2) WPA is granted by the Chairman of Harju County Court or a judge designated by them at a reasoned written request of the Prosecutor General or a prosecutor appointed by them. A judge shall promptly review a submitted request and, by a ruling, grant permission or refuse to do so for justified reasons.

A court may grant permission for the conduct of surveillance activities specified in § 18^1 subsection 3 WPA for a term of up to two months and this term may be extended by two months at a time at the request of the Prosecutor General or a public prosecutor appointed by them.

In cases of urgency, the surveillance activities specified in § 18^1 subsection 3 WPA may be conducted with the permission of a court issued in a format which can be reproduced. Written permission shall be formalised within 24 hours of the commencement of surveillance activities. The person with regard to whom the surveillance activities were conducted shall not be informed thereof.

§ 18^2 WPA provides that for ensuring conspiracy, the witness protection authority has the right, pursuant to the procedure provided by the Police and Border Guard Act:

1) to use covert measures which allow the concealment of the persons who are engaged in the application of witness protection and the purpose of the activities and the ownership of the rooms and means of transport used;
2) to pretend to be a private legal person, a structural entity or a body thereof or a branch of a foreign company;
3) to use undercover agents and persons involved in secret co-operation.

§ 19 WPA provides that the witness protection authority has the right, in order to perform the duties assigned to it by law, to process personal data and set up databases.

The information collected in the course of making a decision on placing a person under witness protection or in the application of witness protection and other mate-

rial related to the application of witness protection shall be stored in a protection file. A separate protection file shall be opened for each protected person. The procedure for keeping and storing protection files shall be established by a regulation of the Minister of the Interior. The information related to witness protection which is not a state secret for the purposes of the State Secrets and Classified Information of Foreign States Act is the information intended for internal use for the purposes of the Public Information Act.

4. The Defence Forces Organisation Act

The Estonian Defence Forces Organisation Act (EDFOA),[20] passed on 19 June 2008 and entered into force on 1 January 2009, provides for the legal status and functions of the Estonian Defence Forces, the organisation of the Defence Forces, the basis for commanding the Defence Forces, and the basis for the use of force by the Defence Forces. The provisions of the Administrative Procedure Act apply to the administrative proceedings prescribed in EDFOA, taking account of the specifications provided for in this Act.

§ 41 EDFOA provides that the security authorities shall cooperate with the Defence Forces upon performance of intelligence and counter-intelligence tasks which concern the Defence Forces to the extent provided by law. The structural units of the Defence Forces and their servants have the right to participate in intelligence and counterintelligence operations relating to the Defence Forces provided that they are involved by the security authorities.

§ 41^1 EDFOA provides that the Military Police of the Estonian Defence Forces may make an enquiry to telecommunications undertaking on the basis specified in § 126^2 clauses (1) 1) and 2) ECCP and in respect of the persons specified in § 126^2 clauses (3) 1) and 2) ECCP to get the following data:

1) the information needed to establish the end-user who is connected to the user identifier used in the electronic communication network, except the data relating to the fact of forwarding a message;
2) to the electronic communications undertaking, the information specified in § 111^1 (2) and (3) ECA which is not mentioned in § 41^1 clause 1 EDFOA.

The authorisation for making the enquiry specified in § 41^1 (1) 2) EDFOA shall be granted by the Prosecutor's Office. The authorisation for making an enquiry shall set out the period during which the request for information must be made.

§ 41^2 EDFOA provides that the Military Police of the Estonian Defence Forces may collect personal information concerning a person who is in military service or wishes to enter the military service by means of surveillance activities specified in

[20] For the text and translation into English of the Act, please see annex.

subsection 126[3] (1) ECCP and by means of an enquiry to the communications undertaking about the information specified in subsections 111[1] (2) and (3) ECA if this is needed for making a decision regarding the access of a person to surveillance information or for employment of a person to a post of military rank in the Military police of the Estonian Defence Forces. Prior written consent of a person is required for the collecting of data provided for in § 41[2] subsection 1 EDFOA or making an enquiry. A person shall be notified of the performance of an act specified in § 41[2] subsection 1 EDFOA with regard to him, and the data collected by means of the act shall be introduced at his request.

5. The Imprisonment Act

The Imprisonment Act,[21] passed on 14 June 2000 and entered into force on 1 December 2000, provides the procedure for and organisation of execution of imprisonment, detention, and custody pending trial, and the definition and conditions of the prison service and service as a prison officer. § 33[1] Imprisonment Act provides that the Prison Department of the Ministry of Justice and the prison may make enquiries to electronic communications undertakings on the basis specified in § 126[2] clauses (1) 1) and 2) ECCP and with regard to the persons specified in § 126[2] clauses (3) 1) and 2) ECCP for obtaining the following data:

1) the data required for the identification of an end-user related to the identification tokens used in the electronic communications network, except the data relating to the fact of transmission of messages;
2) to electronic communications undertakings, the data specified in § 111[1] clauses (2) and (3) ECA and not specified in clause 1) of this section.

The Prosecutor's Office shall grant permission for making the inquiry specified in § 33[1] clause (1) 2) Imprisonment Act. The permission to make inquiries shall set out the period concerning which the request of data is permitted.

§ 33[2] Imprisonment Act provides that the Prison Department of the Ministry of Justice may, with a person's written consent, collect his or her personal data by the surveillance activities specified in § 126[3] (1) ECCP and by the inquiries to electronic communications undertakings concerning the data specified in § 111[1] (2) and (3) ECA, if this is necessary to decide on the access of the person to surveillance information or employment of the person in the Prison Department of the Ministry of Justice or a prison. A person shall be notified of the surveillance activities against them and which are prescribed in § 33[2] subsection 1 Imprisonment Act after making the decision and the data collected by the activities shall be shown to them at their request.

---

[21] For the text and translation into English of the Act, please see annex.

§ 33[2] (1) Imprisonment Act: The Prison Department of the Ministry of Justice and a prison have the right to recruit persons for secret co-operation and use undercover agents in order to conduct surveillance activities, ensure the conducting thereof or collection of information and to use covert measures on the terms and conditions provided for in the Police and Border Guard Act. The head of the Prisons Department of the Ministry of Justice or a prison or an official authorized by them shall authorize the recruitment of a person. The head of the Prisons Department of the Ministry of Justice or a prison shall authorize the use of an undercover agent.

The documents necessary for using covert measures are issued and the necessary amendments in databases and registries are made, at a reasoned request of the head of the Prisons Department of the Ministry of Justice or a prison or an official authorized by them, by an administrative authority or a legal person under whose competence the issue of corresponding documents or making of amendments in the database or register falls.

6. The Aliens Act

The Aliens Act,[22] passed on 9 December 2009 and entered into force on 1 October 2010, regulates the basis for the entry of aliens into Estonia, their temporary stay, residence and employment in Estonia and their legal liability for violation of obligations provided for in this Act. (The Citizen of the European Union Act provides for the legal basis of the temporary stay and residence in Estonia of citizens of the Member States of the EU, citizens of the Member States of the European Economic Area or citizens of the Swiss Confederation and their family members. The Act on Granting International Protection to Aliens provides for the legal basis for the temporary stay, residence and employment in Estonia of applicants for international protection and of those who have been granted protection. The legal basis for the temporary stay, residence, and employment in Estonia of the staff of diplomatic missions and consular posts of foreign states and their family members is provided by treaties and other instruments of international law. The National Defence Act provides for the legal basis for the entry into Estonia, temporary stay, residence, and employment in Estonia of an alien entering Estonia in the framework of international military cooperation.)

§ 31[1] Aliens Act provides that a competent authority specified in § 126[2] (1) ECCP may, with the written consent of the person, collect data about them or evidence regarding the facts that are relevant to the proceedings by surveillance activities specified in § 126[3] (1) ECCP and by an inquiry to a communications undertaking concerning the information provided for in § 111[1] clauses (2) and (3) ECA where that is needed for the issue of an administrative act or performance of an act.

---

[22] For the text and translation into English of the Act, please see annex.

A person shall be notified of the conduct of surveillance activities concerning them after the issue of an administrative act or performance of an act and the data collected by surveillance activities shall be submitted to them for examination at their request.

7. The Status of Members of the Riigikogu Act

Protection of postal items and of messages transmitted through an electronic communication network by or to a member of the *Riigikogu* is provided in § 18^4 of the Status of Members of the Riigikogu Act (SMRA),[23] passed on 14 June 2007 and entered into force on 14 July 2007 (and partially on 1 January 2008 and partially on the day the mandate of the XII Riigikogu began). § 18^4 SMRA provides that any work-related messages that a member of the *Riigikogu* sends or receives through an electronic communication network are protected by immunity. This does not apply when procedural acts under §§ 382^2 (1) and 382^2 (4) ECCP are performed in respect of the member of the *Riigikogu* with the approval of the President of the Tallinn Court of Appeal or the Chancellor of Justice.

8. The Security Act

The Security Act,[24] passed on 8 October 2003 and entered into force on 1 May 2004, provides the conditions and the procedure for the activities of undertakings providing security services (hereinafter *security firms*), the rights and obligations of security guards, the guarantees for security guards, the conditions and the procedure for organizing in-house guarding, the procedure for exercising supervision over the activities of security firms and in-house guarding units, and the liability for violations of this Act. This Act does not apply to authorities and units within the area of government of the Ministry of Defence, the Ministry of Justice or the Ministry of the Interior whose function is to guarantee and organize the guarding and protection of an object. This Act does not apply to the Defence League in respect of objects the guarding and protection of which the Commander of the Defence Forces has assigned to the Defence League. The provisions of the Administrative Procedure Act apply to administrative proceedings prescribed in this Act, taking account of the specifications provided for in this Act.

§ 46^1 Security Act provides that the police may, with the written consent of an applicant for an activity licence, collect personal data concerning the applicant through surveillance activities specified in § 126^3 (1) ECCP and by an enquiry to an electronic communications undertaking with respect to information provided for in § 111^1 clauses (2) and (3) ECA if it is necessary in order to decide on the grant

---

[23] For the text and translation into English of the Act, please see annex.

[24] For the text and translation into English of the Act, please see annex.

of an activity licence which covers the object specified in § 83 National Defence Act. A person shall be notified of the activity prescribed in subsection (1) in respect of them after a decision is made, and they shall be shown upon request, any information collected by the activity.

9. The Securities Market Act

The Securities Market Act,[25] passed on 17 October 2001 and entered into force on 1 January 2002 (and partially on 1 May 2004), regulates the public offer of securities and their admission to trading on regulated securities markets, the activities of investment firms, the provision of investment services, the provision of data reporting services, the functioning of a regulated securities market and a securities settlement system, the exercising of supervision over the securities market and the participants therein as well as the liability thereof. § 230^3 Securities Market Act provides that in order to exercise supervision, the Supervision Authority has the right to obtain information, documents, and explanations from any natural or legal person and from government agencies, supervisory bodies and state and local government databases free of charge. In addition to the provisions of § 230^3 subsection 1 Securities Market Act, the Supervision Authority has the right to make an inquiry under § 230 (3) of the Act to obtain the information provided for in § 111^1 (2) and (3) ECA.

10. The Strategic Goods Act

The Strategic Goods Act,[26] passed on 7 December 2011 and entered into force on 1 January 2012 (and partially on 30 June 2012), establishes a strategic goods control system, regulating the transfer of strategic goods, provision of services related to strategic goods, control over import and end-use of strategic goods and implementation of state supervision in all these fields. § 76 Strategic Goods Act provides that a competent authority specified in § 126^2 (1) ECCP may collect information about a person with the written consent of the person by means of the surveillance activities specified in § 126^3 (1) ECCP and question a communications undertaking about the data provided for in § 111^1 clauses (2) and (3) ECA if this is necessary to decide the conduct of the proceeding prescribed in § 71 clauses (1) 3)–8) Strategic Goods Act and if the commission finds that the applicant or their background, reliability or the data submitted by them is raising reasonable doubt and other options to check them have been depleted. A person shall be notified of the surveillance activities conducted against them after completion thereof and passing

[25] For the text and translation into English of the Act, please see annex.

[26] For the text and translation into English of the Act, please see annex.

the resolution by the commission and may request to examine the data collected by means of surveillance activities in the procedure provided for in the ECCP.

11. The Weapons Act

The Weapons Act,[27] passed on 13 June 2001 and entered into force on 31 March 2002, establishes the legal basis and procedure for the handling of weapons and ammunition, the grant of permission for weapons and ammunition to be used for civilian purposes, the use of weapons and ammunition for civilian purposes and the removal of weapons and ammunition from civilian use, the requirements for firing ranges and field firing ranges, and the basis and procedure for the exercise of state supervision in such areas. The provisions of the Administrative Procedure Act apply to the administrative proceedings prescribed in the Act, taking into account the specifications provided for in the Act.

§ 35^2 Weapons Act provides that if in order to acquire or own a firearm, an acquisition permit or a weapons permit is applied for by an alien who holds an Estonian residence permit or who resides in Estonia on the basis of a residence permit, the police may, with the written consent of the applicant, collect personal data concerning the applicant through surveillance activities specified in § 126^3 (1) ECCP and by an enquiry to an electronic communications undertaking for obtaining information provided for in § 111^1 (2) and (3) ECA if it is necessary in order to decide on the grant of a permit. A person shall be notified of the activity prescribed in Weapons Act § 35^2 subsection 1 relating to them after a decision has been made, and upon request they shall be shown any information collected by the activity.

§ 67^1 Weapons Act provides that the police may, with the written consent of the applicant for an activity licence, collect personal data concerning the applicant through surveillance activities specified in § 126^3 (1) ECCP and by an enquiry to an electronic communications undertaking for obtaining information provided for in § 111^1 (2) and (3) ECA if it is necessary in order to decide on the grant of an activity licence. A person shall be notified of the activity specified in § 67^1 subsection 1 Weapons Act relating to them after a decision has been made, and upon request they shall be shown any information collected by the activity.

G. Statistics on Electronic Communications Interception

The Estonian ECA § 112^1 concerns the notification of the European Commission. According to § 112^1 ECA the communications undertaking must, by 1 February annually, submit the following information concerning the requests

[27] For the text and translation into English of the Act, please see annex.

submitted in accordance with § 112 ECA during the previous calendar year to the Technical Surveillance Authority:

1) the number of requests which resulted in providing information;
2) the period, in days, between the date of preserving the data specified in § 111^1 subsections 2 and 3 ECA and the date of the request;
3) the number of requests where providing information was not possible.

The Technical Surveillance Authority shall submit the information specified in § 112^1 subsection 1 ECA to the European Commission by 1 April each year. The information specified in § 112^1 subsections 1 and 2 ECA shall not contain personal data. The Technical Surveillance Authority shall publish the form for presenting the information specified in § 112^1 subsection 1 ECA on its website.

§ 126^{15} ECCP provides that a Prosecutor's Office shall exercise supervision over the compliance of surveillance activities with the permission provided for in ECCP § 126^4. The committee of *Riigikogu* specified in § 36 Security Authorities Act shall exercise supervision over the activities of surveillance agencies. A surveillance agency shall submit a written report to the committee through the appropriate ministry at least once every three months.

The Ministry of Justice shall publish on its website once a year a report on the basis of the information obtained from surveillance agencies, Prosecutor's Offices and courts, which contains the following information concerning the previous year:

1) number and type of opened surveillance files;
2) number of permissions for surveillance activities by types of surveillance activities;
3) number of persons notified of conduct of surveillance activities and number of persons in the case of whom notification was postponed pursuant to § 126^{13} subsection 4 ECCP for more than one year.

IV. International Cooperation in Criminal Procedure

A. Overview

1. The Code of Criminal Procedure

International cooperation in criminal procedure is the subject of chapter 19 of ECCP.

§ 433 ECCP provides that international cooperation in criminal procedure comprises extradition of persons to foreign states, mutual assistance between states in criminal matters, execution of the judgments of foreign courts, taking over and transfer of criminal proceedings commenced, cooperation with the International

Criminal Court and Eurojust and extradition to Member States of the European Union. International cooperation in criminal procedure shall be effected pursuant to the provisions of ECCP chapter 19 unless otherwise prescribed by the international agreements of the Republic of Estonia, EU legislation or the generally recognised principles of international law. International cooperation in criminal procedure shall be effected pursuant to the provisions of the other chapters of ECCP in so far as this is not in conflict with the provisions of ECCP chapter 19. The requirement of confidentiality shall be complied with in the course of international cooperation in criminal procedure to the extent necessary for the purposes of cooperation. If compliance with the confidentiality requirement is refused, the requesting state shall be immediately notified of such refusal.

2. Judicial authorities competent to engage in international cooperation in criminal procedure

§ 435 ECCP provides that the central authority for international cooperation in criminal procedure in Estonia is the Ministry of Justice, unless otherwise provided by law or international legislation binding on the Republic of Estonia. Courts, the Prosecutors' Offices, the Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Environmental Inspectorate, the Competition Board and the Military Police are the judicial authorities competent to engage in international cooperation in criminal procedure to the extent provided by law and international legislation binding on the Republic of Estonia. If the Penal Code of Estonia is applied to criminal offences which are committed outside the territory of the Republic of Estonia, the Office of the Prosecutor General, which initiates criminal proceedings or verifies the legality and justification of commencement of the criminal proceedings, shall be immediately informed thereof.

3. Prohibition on international cooperation in criminal procedure

§ 436 ECCP provides that the Republic of Estonia refuses to engage in international cooperation if:

1) it may endanger the security, public order or other essential interests of the Republic of Estonia;
2) it is in conflict with the general principles of Estonian law;
3) there is reason to believe that the assistance is requested for the purpose of bringing charges against or punishing a person on account of their race, nationality or religious or political beliefs, or if the situation of the person may deteriorate for any such reasons.

The Republic of Estonia shall not refuse to engage in international cooperation with a Member State of the EU on the ground that the offence is regarded as a political offence, an offence connected with a political offence or an offence inspired

by political motives, unless otherwise provided by law or an international agreement. The Republic of Estonia shall not refuse to engage in international cooperation with a Member State of the EU on the ground that the same kind of tax or duty is not imposed or the same type of taxes, customs or exchange arrangements have not been established in Estonia as in the requesting state. The Republic of Estonia may not refuse international cooperation on the basis of national economic interests, foreign policy interests or other considerations, if this is contrary to an international agreement binding on Estonia.

The Republic of Estonia may refuse international cooperation if it is obvious that a non-EU state does not ensure an adequate level of data protection. The respective decision is made by the Ministry of Justice in coordination with the Ministry of Foreign Affairs, the Data Protection Inspectorate and the Office of the Prosecutor General.

4. Division of expenses relating to international cooperation in criminal procedure

§ 437 ECCP provides that the Republic of Estonia as a requesting and executing state shall bear all the costs arising on its territory from international agreements or other legislation binding on the Republic of Estonia, unless otherwise resolved by agreement with a foreign state.

5. Cooperation with Eurojust

§ 489^1 ECCP provides that cooperation with the EU Judicial cooperation Unit Eurojust shall be carried out pursuant to ECCP unless otherwise provided by EU legislation.

B. Cooperation in Criminal Procedure among Member States of the EU

1. Legal basis for international cooperation with EU Member States

Until 14 March 2019, the provisions of Division 8 of chapter 19 of ECCP on international cooperation in criminal Proceedings applied to international cooperation in criminal procedure based on the EU measures of cooperation in criminal procedure and where the other party to the cooperation has also acceded to the EU measures of cooperation in criminal procedure. Since 15 March 2019, the transmission of personal data to third countries and international organisations in the course of cooperation in criminal proceedings has to comply with the procedure provided for in Division 7 of chapter 4 of the Personal Data Protection Act. ECCP §§ 489^3, 489^4 and 489^5 were repealed.

2. Protection of personal data in an international exchange of data within the framework of cooperation in criminal procedure

§ 489[3] ECCP provided that transmission of personal data to Member States within the framework of cooperation in criminal procedure had to comply with the principles provided for in § 6 Personal Data Protection Act.[28] Processing of personal data received from Member States was permitted only for the purposes for which the data was transmitted. Processing of personal data for a purpose other than that provided for in ECCP § 489[3] subsection 2 was permitted only if this was necessary:

1) in order to detect and combat criminal offences, conduct criminal proceedings or execute punishments;
2) in order to conduct any administrative or court proceedings, if this is directly related to the activities specified in clause 1) of this subsection;
3) in order to prevent serious and imminent threat to public order; or
4) for any other purposes, if the consent of the state which transmitted the data for processing of the personal data for such purpose or proper consent of the data subject exists.

3. Transmission of personal data received from Member States within the framework of cooperation in criminal procedure to competent authorities of third states and international organizations

§ 489[4] ECCP provided that it was permitted to transmit the personal data received from Member States within the framework of cooperation in criminal procedure to third states or international organizations only when:

1) it was necessary in order to detect and combat criminal offences, conduct criminal proceedings or execute criminal punishments;
2) the authority or organization which received the data was responsible for detection of and combating criminal offences, conduct of criminal proceedings or execution of punishments;
3) the foreign state which transmitted the personal data had given proper consent for the transmission thereof; and
4) the state or international organization which received the personal data ensured sufficient protection thereof.

Transmission of personal data received from Member States to third states or international organizations without the consent specified in § 489[4] clause (1) 3) ECCP was permitted only if it was necessary in order to prevent serious and imminent threat to public order or other essential interests and it was impossible to ob-

[28] For the text and translation into English of the Act, please see annex.

tain prior consent on time. A competent authority of the Member State which transmitted personal data had to be immediately notified of such data exchange.

As an exception to the provisions of § 489[4] clause (1) 4) ECCP, transmission of personal data received from Member States to third states or international organizations was permitted if:

1) it was necessary for the protection of the legitimate interests of data subjects or substantial public interests; or
2) the states or international organizations which received personal data ensured sufficient protection of personal data in compliance with Estonian law.

4. Transmission of personal data received from Member States within the framework of cooperation in criminal procedure to private persons

§ 489[5] ECCP provided that it was permitted to transmit the personal data received from Member States within the framework of cooperation in criminal procedure to private persons only if the Member State which had transmitted the data had granted proper consent for the transmission thereof and transmission of personal data was in compliance with the legitimate interests of the data subject. Transmission of personal data to private persons was permitted, if it was necessary:

1) in order to perform the functions assigned to a competent authority of Estonia by law;
2) in order to detect and combat criminal offences, conduct criminal proceedings or execute punishments;
3) in order to prevent serious and imminent threat to public order; or
4) in order to avoid violation of the rights of a person.

When personal data was transmitted to a private person, the permitted purpose for the use thereof had to be explained to them.

The Personal Data Protection Act regulation currently in force reads as follows:

§ 46. General terms and conditions of transmission of personal data to third countries and international organisations

(1) It is permitted to transmit personal data to third countries or international organizations only in the case all the following terms and conditions are met:

1) transmission is necessary for prevention, detection or processing of offences or execution of punishments;

2) personal data are transmitted to the controller in any third country or international organisation that is competent to prevent, detect and proceed offences or execute punishments;

3) consent of another Member State of the European Union for further use of the data, if the data transmitted have been received from this Member State;

4) the European Commission has adopted a decision pursuant to Article 36 of Directive (EU) 2016/680 of the European Parliament and Council on adequacy of the

protection or, in the absence of such decision, the safeguards specified in § 47 of this Act or in the absence thereof the exception specified in § 48 of this Act is applied;

5) it is ensured upon transmission of personal data that the controller that transmits data has given an earlier consent for further transmission of personal data to another third country or international organization.

(2) If the authorisation specified in clause (3) 1) of this section for transmission of personal data cannot be obtained in due time and transmission of personal data is necessary to prevent any immediate and serious threats to the public order of the state or any third country or to protect essential interest of the state, the personal data may be transmitted without the authorisation specified in clause (3) 1) of this section. The competent authority of the Member State of the European Union which transmitted personal data shall be immediately notified of the data exchange provided for in this subsection.

(3) When giving the consent specified subsection clause (1) 5) of this section, the controller or processor shall inter alia take into consideration the gravity of the offence, the purpose of initial transmission of personal data and the protection level of personal data in this third country or international organization where the personal data are sent.

(4) If the European Commission has adopted the decision specified in Article 36(5) of Directive (EU) 2016/680 of the European Parliament and of the Council, personal data may be transmitted to third countries or international organizations pursuant to §§ 47 and 48 of this Act.

§ 47. Transmission of personal data subject o application of appropriate safeguards

In the absence of the decision of the European Commission specified in clause 46 (1) 4) of this Act on the adequacy of the protection, personal data may be transmitted to third countries or international organizations in the following cases:

1) the appropriate safeguards taken for the protection of personal data are provided for in a legally binding legal instrument;

2) the controller has assessed all the circumstances relating to transmission of personal data and found that all the safeguards appropriate from the point of view of protection of personal date have been taken.

§ 48. Transmission of personal data in exceptional cases

(1) If the absence of the decision of the European Commission specified in clause 46 (1) 4) of this Act or in the absence of appropriate safeguards specified in § 47 of this Act, transmission of personal data to third countries or international organizations is permitted if this is required in order to:

1) protect the rights and freedoms of data subjects or any other persons;

2) protect the legitimate interests of data subjects;

3) prevent immediate and serious threat to public order;

4) prevent, detect or process offences or execute punishments; or

5) compile, submit or defend a particular legal claim related to the aim of prevention, detection or processing of a particular offence or enforcement of punishment.

(2) If the rights of the data subject outweigh the interest provided for in clauses (1) 4) and 5) of this section, transmission of personal data shall not be permitted.

§ 49. Transmission of personal data to recipients in third countries

Personal data may be transmitted directly to a recipient in any third country if all the following conditions are met:

1) the transmission is strictly necessary for performance of the tasks of the law enforcement authority, which transmits the personal data, for the purpose of prevention, detection and proceeding of offences or execution of punishments;

2) the public interest outweighs the rights and freedoms of the data subject;

3) the transmission of personal data to an agency of any third country, which is competent to prevent, detect and process the offence or execute the punishment, is not effective or appropriate;

4) the agencies of third countries which are competent to prevent, detect and proceed offences or execute punishments shall be notified immediately, except in the case this is not effective or appropriate;

5) the recipient shall be notified of the specific purpose of processing of personal data and is directed to process personal data only for the specified purpose.

5. Scope of assistance

§ 489[6] ECCP provides that on the basis of the provisions of the EU cooperation in criminal procedure, recognition and execution of a court judgment or decision of another authority is permitted regardless of the punishability of the act according to the law of Estonia, if imprisonment of at least three years is prescribed as a maximum in the requesting state for commission of the following criminal offences:

1) participation in a criminal organization;
2) terrorism;
3) trafficking in human beings;
4) sexual exploitation of children and child pornography;
5) illicit trafficking in narcotic drugs and psychotropic substances;
6) illicit trafficking in weapons, ammunition and explosives;
7) corruption;
8) fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests;
9) money laundering;
10) counterfeiting currency;
11) computer-related crime;
12) environmental crime, including illicit trafficking in endangered animal species and endangered plant species and varieties;
13) facilitation of unauthorised entry and residence;
14) manslaughter, causing serious damage to health;
15) illicit trade in human organs and tissue;
16) kidnapping, unlawful deprivation of liberty and hostage taking;
17) racism and xenophobia;

18) organized or armed theft or robbery;
19) illicit trafficking in cultural goods, including antiques and works of art;
20) swindling;
21) extortion;
22) piracy and counterfeiting of products and trafficking therein;
23) forgery of administrative documents and trafficking therein;
24) counterfeiting and forgery of means of payment;
25) illicit trafficking in hormonal substances and other growth promoters;
26) illicit trafficking in nuclear or radioactive materials;
27) trafficking in stolen vehicles;
28) rape;
29) arson;
30) criminal offences which fall within the jurisdiction of the International Criminal Court;
31) unlawful seizure of aircraft or ships;
32) sabotage.

In the case of criminal offences other than the offences specified in § 489^6 subsection 1 ECCP, recognition and execution of a court judgment or decision of other authorities is permitted on the basis of the provisions of the EU cooperation in criminal procedure only if the respective act is punishable as a criminal offence in Estonia. On the basis of the provisions of the EU cooperation in criminal procedure, recognition and execution of a court judgment or decision of other authorities is permitted if there are no grounds for refusal provided for in § 436 ECCP and the requirements provided for in § 477 ECCP are met.

§ 50. Notification of Estonian Data Protection Inspectorate and documentation of transmission of personal data

(1) The controller or processor shall provide an overview to the Estonian Data Protection Inspectorate of transmission of personal data pursuant to clause 47 2) and § 49 of this Act at least once a year.

(2) If personal data is transmitted pursuant to clause 47 2), subsection 48 (1) or § 49 of this Act, the controller or processor shall document such transmission, including the date and time of transmission, the details of the receiving competent authority, the explanation of transmission and the personal data transmitted.

(3) At the request of the Estonian Data Protection Inspectorate, the controller or processor shall make the information specified in subsection (2) of this section available to it.

6. Proceedings for requests received from EU Member States

§ 489^8 ECCP provides that the central authority for EU cooperation in criminal procedure is the Ministry of Justice, unless otherwise provided for in ECCP.

The Ministry of Justice shall verify whether the request received is in compliance with the requirements and has the required supporting documents and shall immediately communicate the request on the basis of the content thereof to the Office of the Prosecutor General or a court.

If a request for assistance is submitted through Eurojust, the Eurojust's National Member for Estonia shall verify whether the request for assistance meets the requirements and whether compliance with the request for assistance is admissible and possible and communicate the request to the Estonian competent judicial authority for execution. A copy of the request shall be sent to the Office of the Prosecutor General and the Ministry of Justice.

The surrender of or refusal to surrender a person sentenced to imprisonment shall be decided by a court.

7. Methods of submission of certificates and requests

§ 489^{17} ECCP provides that the certificates and requests specified in ECCP Division 9 shall be communicated to requesting states by post, electronic mail or in another format which can be reproduced in writing. The certificates and requests specified in ECCP Division 9 are prepared in the Estonian language and they are translated into the languages determined by the executing state by the authority competent to submit the certificates and requests. Judgments shall not be translated into the language determined by the executing state.

C. European Investigation Order

1. European Investigation Order and access to communications data in Estonian legislation

a) Overview

ECCP amendments, entered into force on 6 July 2017, provided in Division 9, subdivision 1^2, are applied only to those Member States of the EU which have transposed Directive 2014/41/EU of the European Parliament and on the Council into their national law. There are three sub-subdivisions in this Subdivision 1^2: Sub-subdivision 1: General Provisions; Sub-subdivision 2: Proceedings for Recognition and Execution of European Investigation Orders; Sub-subdivision 3: Issue of European Investigations Orders to Member States of the European Union.

§ 489^{37} ECCP provides that the European Investigation Order is a request which is issued or validated by a judicial authority of an EU Member State for performance of a procedural act in another Member State to obtain evidence or transfer or deposit the evidence located in another Member State in order to prevent the de-

struction, transformation, moving, transfer or disposal of the evidence. This Section of General Provisions does not apply to:

1) activities of interstate investigation teams set up pursuant to § 471 ECCP and gathering of evidence within the framework thereof;
2) co-operation with the Kingdom of Denmark and Republic of Ireland in criminal proceedings.

b) Breakdown of costs

§ 489[38] ECCP provides that Estonia as a requesting and executing state shall bear all the costs which are related to the execution of an European Investigation Order on its territory, unless otherwise provided for in this section. As an executing state if the costs associated with the execution of a European Investigation Order are exceptionally high, Estonia may send information about the costs to the issuing authority and consult it on whether and how the costs could be shared or the European Investigation Order modified. An issuing authority may decide to:

1) bear a share of the costs which are deemed to be exceptionally high by the executing state; or
2) withdraw the European Investigation Order in part or in whole.

Estonia as the requesting state shall bear the costs, if these costs:

1) are related to transfer or surrender of persons whose personal liberty is restricted in the cases specified in §§ 489[39] and 489[40] ECCP;
2) are the costs of transcription, decoding or decrypting of messages sent through intercepted telecommunication networks and incurred in the case specified in § 489[43] subsection 4 ECCP.

c) Cross-border surveillance

§ 489[42] ECCP provides that if a European Investigation Order is issued for cross-border surveillance, the provisions of § 472 ECCP apply with the specifications provided for in this Subdivision.

d) Interception or covert observation of information

§ 489[43] ECCP provides that if a European Investigation Order is issued for interception or covert observation of messages transmitted using public electronic communications networks or information communicated by any other means, the provisions of § 126[7] ECCP apply.

If a European Investigation Order is issued for interception or covert observation of messages transmitted using public electronic communications networks with the technical assistance of another Member State and if several EU Member States are

able to provide all the technical assistance required for interception or covert observation, Estonia shall issue the European Investigation Order only to one Member State, preferring the one on whose territory the person to be intercepted or covertly observed is located currently or will be in the future.

A European Investigation Order shall indicate why the information specified in § 489[43] subsection 1 ECCP is relevant in criminal proceedings. If a European Investigation Order is issued for interception or covert observation of messages transmitted using public electronic communications networks with the technical assistance of another Member State, the European Investigation Order shall also specify the following:

1) information needed to identify the person to be intercepted or covertly observed;
2) requested duration of interception or covert observation;
3) other technical information required for execution of the European Investigation Order.

The exact procedure for interception or covert observation shall be agreed between the competent authorities of the requesting state and executing state. A European Investigation Order issued for interception or covert observation of messages transmitted using public electronic communications networks may be executed according to an agreement in the following manner:

1) by forwarding the messages transmitted using public electronic communications networks immediately to the requesting state; or
2) by recording the messages transmitted using public electronic communications networks and intercepted or covertly observed and by forwarding the recorded information to the requesting state.

A requesting authority may request, during the issue or execution of a European Investigation Order, transcription, decoding or decrypting of recordings of messages transmitted using public electronic communications networks, if it has good reasons and if the executive authority agrees.

e) Notification of interception and covert observation of messages transmitted using public electronic communications networks

§ 489[44] ECCP provides that where, during the execution of a European Investigation Order, a preliminary investigation judge authorises, on the basis of § 126[7] ECCP, interception or covert observation of messages transmitted using public electronic communications networks with respect to a person or device located on the territory of another Member State (hereinafter *notified Member State*) from which no technical assistance is needed to carry out the interception or covert observation, a Prosecutor's Office shall notify the competent authorities of the notified Member State of interception or covert observation:

1) prior to the interception or covert observation in the cases where the Prosecutor's Office knows at the time of applying for an authorisation for interception or covert observation that the person or device subject to interception or covert observation is or will be at that moment or at the time of interception or covert observation on the territory of the notified Member State;
2) during the interception or covert observation or after the interception or covert observation when the Prosecutor's Office has obtained information that the person or device in question is or has been on the territory of the notified Member State.

Where a competent authority of the notified Member State notifies the Prosecutor's Office that interception or covert observation would not be authorised in the notified Member State in a similar domestic case, the Prosecutor's Office shall:

1) terminate the interception or covert observation on the territory of the notified Member State; and
2) not use as evidence the information which was obtained as a result of interception or covert observation during the time the person or device in question was on the territory of the notified Member State, except under the conditions specified by the competent authority of the Member State which have been justified by the notified Member State.

When another Member State has notified the Prosecutor's Office of interception or covert observation of messages transmitted using public electronic communications networks with respect to a person or device located on the territory of Estonia,and interception or covert observation would not be authorised in Estonia in a similar domestic case, the Prosecutor's Office shall notify the submitting Member State immediately but at the latest 96 hours after receipt of the notification of that:

1) the interception or covert observation may not be carried out or shall be terminated; and
2) the information obtained as a result of the interception or covert observation while the person or device in question was on the territory of Estonia may not be used or may be used under the conditions specified by the Prosecutor's Office, and justify those conditions.

The format of the notification specified in § 489^{44} subsection 1 ECCP shall be established by a regulation of the minister responsible for the area.

2. Proceedings for recognition and execution of European Investigation Orders

a) Recognition and execution of European Investigation Orders

§ 489^{46} ECCP provides that a Prosecutor's Office is competent to recognise, conduct proceedings in and ensure the execution of a European Investigation Or-

der. The Prosecutor's Office may obligate an investigative body to execute a European Investigation Order. Within seven days after receipt of a European Investigation Order, the Prosecutor's Office shall notify the competent authority of the requesting Member State thereof. The format of the notification specified in § 489[46] subsection 2 ECCP shall be established by a regulation of the minister responsible for the area.

Unless a European Investigation Order was issued or confirmed by a judge, court, preliminary investigation judge or prosecutor of a requesting Member State, the Prosecutor's Office shall return the European Investigation Order to the requesting Member State. If deficiencies or obvious inaccuracies are found in a European Investigation Order, the Prosecutor's Office shall consult the requesting state about elimination of the deficiencies.

Execution of a European Investigation Order shall be based on the instructions described by the requesting state in the European Investigation Order, except to the extent compliance with the instructions would be in conflict with the general principles of Estonian law.

A procedural act requested in a European Investigation Order shall be performed on the same basis and as quickly as a domestic procedural act performed on the same basis and the deadlines provided for in § 489[47] ECCP apply. If performance of a procedural act is requested by a European Investigation Order for depositing evidence, the Prosecutor's Office may shorten the duration of depositing of the evidence prescribed in the European Investigation Order, if necessary, after consulting the competent authorities of the requesting Member State. The Prosecutor's Office shall notify the competent authority of the requesting state before termination of depositing of the evidence.

b) Terms for recognition and execution of European Investigation Orders

§ 489[47] ECCP provides that the decision on the recognition of the European Investigation Order must be made immediately but not later than 30 days after receipt. If the European Investigation Order was issued for depositing of evidence, the decision on recognition of the European Investigation Order must be made, if possible, within 24 hours of receipt. If it is impossible to decide on recognition during the term provided for in § 489[47] subsection 1 ECCP, the Prosecutor's Office shall immediately inform the competent authority of the requesting state thereof and state the reasons for the delay and the additional time required for making the final decision which may not be longer than 30 days.

If none of the circumstances provided for in § 489[49] ECCP for postponement exist, the procedural act requested in the European Investigation Order must be performed and the evidence gathered must be transferred to the requesting state immediately but not later than 90 days after making the decision on the basis of

§ 489[47] subsections 1 and 2 ECCP on recognition of the European Investigation Order. If it is impossible to perform the procedural act requested in the European Investigation Order during the term provided for in § 489[47] subsection 3 ECCP, the Prosecutor's Office shall immediately notify the competent authorities of the requesting state thereof and state the reasons for the delay and consult the competent authorities of the requesting state about the time of execution of the European Investigation Order.

c) Transfer of evidence

§ 489[48] ECCP provides that the Prosecutor's Office shall immediately transfer to the requesting Member State the evidence obtained on the basis of the European Investigation Order which is in the possession of the Prosecutor's Office or investigative body, and the evidence which has been obtained as a result of the execution of the European Investigation Order. Transfer of evidence may be suspended until the end of the appeal if the procedural act by which the evidence was obtained has been contested pursuant to the EECP. Transfer of evidence shall not be suspended if sufficient reasons are stated in the European Investigation Order justifying the immediate transfer of evidence as essential for proper performance of the procedural act or protection of the rights of individuals, except if transfer of evidence may result in serious and irreversible violation of the rights of persons. In agreement with the competent authorities of the requesting Member State, the Prosecutor's Office may temporarily transfer the evidence requested provided that the evidence shall be returned to Estonia as soon as it is no longer required in the requesting Member State, or at any other time which is agreed upon between the Prosecutor's Office and the competent authorities of the requesting Member State.

d) Postponement of the execution of European Investigation Orders

§ 489[49] ECCP provides that the Prosecutor's Office may postpone the execution of a European Investigation Order if:

1) the execution of the European Investigation Order may damage ongoing criminal proceedings in Estonia;
2) the objects, documents or information required for performance of a procedural act on the basis of the European Investigation Order are already being used in other proceedings.

The Prosecutor's Office shall notify the competent authorities of the requesting state on the basis of § 489[49] subsection 1 ECCP of postponement of the execution of a European Investigation Order and the duration thereof.

e) Adjustment of the execution of European Investigation Orders

§ 489[50] ECCP provides that instead of the procedural act requested in the European Investigation Order, a procedural act of another type may be performed, if this is suitable for achieving the objective pursued, and:

1) the procedural act stated in the European Investigation Order is not prescribed in the ECCP; or
2) performance of the procedural act requested in the European Investigation Order is not permitted pursuant to Estonian law in the case of the offence specified in the European Investigation Order.

It is not permitted to perform a procedural act of another type instead of the procedural act requested in the European Investigation Order if performance of the following procedural acts was requested:

1) forwarding of such information or evidence which is in the possession of the Prosecutor's Office or investigative body and the obtaining of which would have been possible within the framework of criminal proceedings or the European Investigation Order pursuant to subsection 32 (2) ECCP;
2) questioning of a witness, expert, specialist, victim, suspect, accused or third person on the territory of Estonia;
3) a procedural act provided for in subsection 90[1] (1) ECCP;
4) a procedural act the performance of which does not prejudice the fundamental rights of persons.

Before adjustment of the execution of a European Investigation Order pursuant to this section, the Prosecutor's Office shall consult the competent authorities of the requesting Member State and notify them of the need to perform a procedural act of another type.

f) Refusal to execute a European Investigation Order

§ 489[51] ECCP provides that execution of a European Investigation Order may be refused in part or in full in addition to the provisions of § 436 ECCP if:

1) a person with respect to whom performance of a procedural act is requested enjoys immunity in the Republic of Estonia or privileges prescribed by an international agreement;
2) it is evident on the basis of a European Investigation Order that execution of the Investigation Order is not permitted because the person has been finally convicted or acquitted on the same charges or, in the case of a judgment of conviction, the imposed punishment has been served or execution of the punishment cannot be ordered pursuant to the legislation of the state which issued the European Investigation Order;

3) the procedural act requested in the European Investigation Order is not permitted pursuant to Estonian law in the case of the offence on the basis of which the European Investigation Order was issued, except for the procedural acts provided for in § 489[50] subsection 2 ECCP, if the European Investigation Order was issued within the framework of the criminal proceedings of the requesting state;
4) the European Investigation Order is related to an offence which was allegedly committed outside the territory of the requesting and, in part or in full, on the territory of the Republic of Estonia, and the act on the basis of which the European Investigation Order was issued is not punishable in Estonia;
5) the act on the basis of which the European Investigation Order was issued is not punishable in Estonia, except in the case of an offence specified in § 489[6] subsection 1 ECCP or if performance of the procedural acts specified in § 489[50] subsection 2 ECCP is requested in the European Investigation Order.

Before refusal to execute a European Investigation Order on the basis of § 489[51] subsection 1 ECCP, the Prosecutor's Office shall consult the competent authorities of the requesting state and notify them of refusal to execute the European Investigation Order.

3. Issue of European Investigation Orders to Member States of the EU

§ 489[52] ECCP provides that the Prosecutor's Office in pre-trial proceedings and the court in the case of court proceedings is competent to issue a European Investigation Order. The European Investigation Order is issued and submitted only if:

1) the issue of a European Investigation Order is necessary for the achievement of the objectives of criminal proceedings and proportionate taking into account the rights of the suspects and accused;
2) the procedural act requested by the European Investigation Order could be performed under the same terms and conditions in domestic criminal proceedings.

If the European Investigation Order is issued for depositing of evidence, the European Investigation Order shall indicate whether the evidence shall be returned to Estonia or it should stay in the possession of the executing state, and the duration for the depositing of evidence or the estimated date of submission of a request for transfer of evidence. If a European Investigation Order delivered for execution is annulled, the competent authority of the executing state shall be immediately notified thereof. The format of a European Investigation Order shall be established by a regulation of the minister responsible for the area.

V. Conclusions

The aim of the legislation that was in force in 2018 was to ensure that state agencies were entitled to use necessary methods of interception in order to intercept the content of electronic communications. According to (legal) practitioners, the legislation was mostly considered to be adequate and sufficient. Cross-border cooperation, however, was considered insufficient due to slow responses from partner states in dealing with the compulsory procedures they were required to comply with. The Estonian Ministry of Justice has built up a statistics database. According to the yearbook of the Estonian Prosecutor's Office,[29] Estonia received 83 MLA-requests and issued 52 MLA-requests to foreign countries in 2017. According to the comments of practitioners, a few of these requests concerned the interception of the content of electronic communications.

The legislation and the practice of its implementation is continually being analysed and improved. The changes made in 2019 were illustrated with examples that were added in the process of editing. It is considered important that the principle of proportionality and necessity are always adhered to. According to the Supreme Court (of Estonia),[30] even in the case of the re-processing of data stemming from earlier surveillance activity in the second instance, *ex post* control over the legality of the surveillance activity and compliance with the *ultima ratio* principle must be ascertained.

The issues raised in practice have led the Estonian Supreme Court to refer the following questions to the Court of Justice of the European Union for a preliminary ruling:[31]

1. Is Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, in conjunction with Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights of the European Union, to be interpreted as meaning that in criminal proceedings the access of state authorities to data making it possible to establish the start and end point, the date, the time and the duration, the type of communications service, the terminal used and the location of use of a mobile terminal in relation to a telephone or mobile telephone communication of a suspect constitutes so serious an interference with the fundamental rights enshrined in those articles of the Charter that that access in the area of prevention, investigation, detection and prosecution of criminal offences must be re-

---

[29] http://www.prokuratuur.ee/et/prokuratuuri-aastaraamat-2017/rahvusvaheline-koostoo

[30] Judgments of the Supreme Court of Estonia RKKKo 3-1-1-10-11, p. 19; RKKKo 3-1-1-14-14, p. 801; RKKKo 3-1-1-92-13, p. 8; RKKKo 3-1-1-14-14, p. 800.

[31] Request for a preliminary ruling from the Riigikohus (Estonia) lodged on 29 November 2018 – H. K. v Prokuratuur (Case C-746/18). Official Journal of the European Union. 2019/C 54/10; 11.2.2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CN0746&from=EN

stricted to the fighting of serious crime, regardless of the period to which the retained data to which the State authorities have access relate?

2. Is Article 15(1) of Directive 2002/58/EC, on the basis of the principle of proportionality expressed in the judgment of the Court of Justice of 2 October 2018 in Case C-207/16, paragraphs 55 to 57, to be interpreted as meaning that, if the amount of data mentioned in the first question, to which the State authorities have access, is not large (both in terms of the type of data and in terms of its temporal extent), the associated interference with fundamental rights is justified by the objective of prevention, investigation, detection and prosecution of criminal offences generally, and that the greater the amount of data to which the State authorities have access, the more serious the criminal offences which are intended to be fought by the interference must be?
3. Does the requirement mentioned in the judgment of the Court of Justice of 21 December 2016 in Joined Cases C-203/ 15 and C-698/15, second point of the operative part, that the data access of the competent State authorities must be subject to prior review by a court or an independent administrative authority mean that Article 15(1) of Directive 2002/ 58/EC must be interpreted as meaning that the public Prosecutor's Office which directs the pre-trial procedure, with it being obliged by law to act independently and only being bound by the law, and ascertains the circumstances both incriminating and exonerating the accused in the pre-trial procedure, but later represents the public prosecution in the judicial proceedings, may be regarded as an independent administrative authority?"

The Court of Justice of the European Union has yet to provide its answer to these questions. The decision is expected to be of consinderable significance for future practice.

In order to give a more precise overview, more detailed statistical data is needed, as well as deeper knowledge that comes from more practice in the field. The type of data required for this is also not in the public domain.

Annex

Bibliography

European e-Justice Portal. Member State law – Estonia, available at https://e-justice.europa.eu/content_member_state_law-6-ee-en.do?member=1

The Yearbook of the Estonian Prosecutor's Office 2017, available at http://www.prokuratuur.ee/et/prokuratuuri-aastaraamat-2017/rahvusvaheline-koostoo

Official Journal of the European Union. 2019/C 54/10, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CN0746&from=EN

Legal Acts

– *Aliens Act:*
https://www.riigiteataja.ee/akt/117052018002. Translation into English: https://www.riigiteataja.ee/en/eli/521052018002/consolide

– *Code of Criminal Procedure:*
https://www.riigiteataja.ee/akt/131052018022. Translation into English: https://www.riigiteataja.ee/en/eli/506062018001/consolide

– *Code of Misdemeanour Procedure:*
https://www.riigiteataja.ee/akt/130122017022. Translation into English: https://www.riigiteataja.ee/en/eli/509012018006/consolide

– *The Constitution of the Republic of Estonia:*
https://www.riigiteataja.ee/akt/115052015002. Translation into English: https://www.riigiteataja.ee/en/eli/521052015001/consolide

– *Customs Act:*
https://www.riigiteataja.ee/akt/111012018014. Translation into English: https://www.riigiteataja.ee/en/eli/504062018001/consolide

– *Defence Forces Organisation Act:*
https://www.riigiteataja.ee/akt/105052017003. Translation into English: https://www.riigiteataja.ee/en/eli/520062017002/consolide

– *Electronic Communications Act:*
https://www.riigiteataja.ee/akt/122052018003. Translation into English: https://www.riigiteataja.ee/en/eli/530052018001/consolide

– *Imprisonment Act:*
https://www.riigiteataja.ee/akt/109032018019. Translation into English: https://www.riigiteataja.ee/en/eli/512032018002/consolide

– *Penal Code:*
https://www.riigiteataja.ee/akt/130122017029. Translation into English: https://www.riigiteataja.ee/en/eli/509012018005/consolide

– *Personal Data Protection Act:*
https://www.riigiteataja.ee/akt/113032019002. Translation into English: https://www.riigiteataja.ee/en/eli/523012019001/consolide

– *Police and Border Guard Act:*
https://www.riigiteataja.ee/akt/106072017006. Translation into English: https://www.riigiteataja.ee/en/eli/515092017001/consolide

– *Security Authorities Act:*
https://www.riigiteataja.ee/akt/105052017002. Translation into English: https://www.riigiteataja.ee/en/eli/521062017015/consolide

– *Taxation Act:*
https://www.riigiteataja.ee/akt/103042018006. Translation into English: https://www.riigiteataja.ee/en/eli/516042018001/consolide

– *Status of Members of the Riigikogu Act:*
https://www.riigiteataja.ee/akt/121062016022. Translation into English: https://www.riigiteataja.ee/en/eli/523082017002/consolide

– *Security Act:*
https://www.riigiteataja.ee/akt/103032017027. Translation into English: https://www.riigiteataja.ee/en/eli/521062017007/consolide

– *Securities Market Act:*
https://www.riigiteataja.ee/akt/130122017043. Translation into English: https://www.riigiteataja.ee/en/eli/527022018002/consolide

– *State Secrets and Classified Information of Foreign States Act:*
https://www.riigiteataja.ee/akt/105052017005. Translation into English: https://www.riigiteataja.ee/en/eli/519062017007/consolide

– *Strategic Goods Act:*
https://www.riigiteataja.ee/akt/112032015048. Translation into English: https://www.riigiteataja.ee/en/eli/501022016001/consolide

– *Weapons Act:*
https://www.riigiteataja.ee/akt/109032018009. Translation into English: https://www.riigiteataja.ee/en/eli/512032018001/consolide

– *Witness Protection Act:*
https://www.riigiteataja.ee/akt/129062012046. Translation into English: https://www.riigiteataja.ee/en/eli/530122013001/consolide

Judgments of the Supreme Court of Estonia

RKKKo 3-1-1-10-11, p. 19

RKKKo 3-1-1-14-14, p. 801

RKKKo 3-1-1-92-13, p. 8

RKKKo 3-1-1-14-14, p. 800

France*

National Rapporteur:
Estelle De Marco

* This report reflects legislation and case law as of February 2019.

Contents

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Public Authorities with Powers of Electronic Communications Interception

Several legal regimes organise the interception and the collection of electronic communications under French law. However, comprehensive statistics are not consistently available.

1. Legal regimes organising the interception and the collection of electronic communications

Under French law, electronic communications are defined as "emissions, transmissions or reception of signs, signals, writings, images or sounds, by electro-magnetic means."[1]

The formula "electronic communications" has replaced the term "telecommunications" according to a law of 9 July 2004.[2] Therefore, where French law still mentions the term of "telecommunications," this notion has to be understood as "electronic communications."[3]

The interception of electronic communications is not provided for as such. French law distinguishes between several types of communications, which may be intercepted or accessed by judicial institutions and/or administrative services following different kinds of procedures, mainly within the framework of the application of either (repressive) penal law, or State security law (which includes the prevention of terrorism, of organised crime, and of organised delinquency). Most of these procedures under State security law were established by law n° 2015-912 of 24 July 2015[4] and its implementing decrees,[5] and later modified in 2015,[6] 2016,[7]

---

[1] Art. L. 32-1 of the Post and Electronic Communications Code (PECC).

[2] Law n°2004-669 of 9 July 2004; see also Court of Cassation, criminal chamber, 8 July 2015, available at http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4696

[3] The most important change in this regard is due to Law n° 2016-731 of 3 June 2016 which replaces the wording "telecommunication" with the wording "electronic communication" in several articles (but not all) of the Penal Code and of the Penal Procedure Code, including provisions related to electronic communication intercept.

[4] Law n° 2015-912 of 24 July 2015 relating to intelligence entered into force October 2015, JORF n° 0171 of 26 July 2015, p. 12735, text n° 2; legislative dossier available at http://www.senat.fr/dossier-legislatif/pjl14-424.html. Its entry into force was scheduled

2017[8] and 2018.[9] Additionally, some traffic data may be accessed by the national authority for information systems' security (ANSSI) for the purpose of the prevention of attacks on a list of automated data processing systems, and by an independent public authority called HADOPI in relation to of the prosecution of one particular infringement to the Intellectual Property Code.[10]

These types of communications and the legal regimes governing their interception or collection are the following:

- Electronic correspondence (during its transmission). These communications receive strong legal protection and may only be intercepted under strict conditions (which have, however, been relaxed since 2012). Electronic correspondence interceptions are organised by repressive penal law[11] and State security law.[12]
- Stored electronic correspondence. Correspondence stored by means of electronic communications can be accessed under certain conditions by means of an electronic identifier, for the purposes of penal repressive law.[13] This possibility, established in June 2016, is not explicitly established for the purpose of intelligence investigations. However, intelligence services are entitled to access "electronic communications services connection data" retained by electronic commu-

---

the day after the publication of a decree nominating the President of a new established "National Commission for intelligence techniques control," which replaces the current "National Commission for security intercepts control." This decree was published on 2 October 2015 (Decree of 1 October 2015 on the composition of the National Commission for intelligence techniques control/*Décret du 1er octobre 2015 relatif à la composition de la Commission nationale de contrôle des techniques de renseignement*), JORF n°0228 of 2 October 2015, p. 17882, text n° 26.

[5] Decree n° 2015-1185 of 28 September 2015 (portant désignation des services spécialisés de renseignement), JORF n° 0225 of 29 September 2015 p. 17344, text n°1; Decree n° 2016-67 of 29 January 2016, JORF n° 0026 of 31 January 2016, text n° 2; Decree n° 2016-1772 of 20 December 2016, JORF n° 0296 of 21 December 2016, text n° 2; Decree n° 2017-36 of 16 January 2017 JORF n° 0014 of 17 January 2017; Decree n° 2017-749 of 3 May 2017, JORF n° 0106 of 5 May 2017, text n° 92; Decree n° 2018-378 of 22 May 2018, JORF n° 0116 of 23 May 2018, text n° 13; Decree n° 2018-543 of 29 June 2018, text n° 28; JORF n° 0149 of 30 June 2018, text n° 2.

[6] Law n° 2015-1556 of 30 November 2015, JORF n° 0278 of 1 December 2015, p. 22185, text n° 1.

[7] Law n° 2016-731 of 3 June 2016, JORF n° 0129 of 4 June 2016, text n° 1; Law n° 2016-987 of 21 July 2016, JORF n° 0169 of 22 July 2016, text n° 2.

[8] Law n° 2017-55 of 20 January 2017, JORF n° 0018 of 21 January 2017, text n° 2; Law n° 2017-258 of 28 February 2017, JORF n° 0051 of 1st March 2017, text n° 3; Law n° 2017-1510 of 30 October 2017, JORF n° 0255 of 31 October 2017, text n° 1; Decree n° 2017-1095 of 14 June 2017, JORF n° 0139 of 15 June 2017, text n° 1.

[9] Law n° 2018-607 of 13 July 2018, JORF n° 0161 of 14 July 2018, text n° 1.

[10] See below for further details.

[11] Arts. 100 *et seq*. and 706-95 PPC.

[12] Arts. L. 852-1 *et seq*. ISC.

[13] Arts. 706-95-1 to 706-95-3 PPC, created by Law n° 2016-731 of 3 June 2016.

nication operators,[14] which might enable these services, in practice, to use any gathered electronic passwords. In such circumstance, they would be obliged to follow the procedure established for correspondence interception.[15]

- Stored or real-time created content data. Procedures allowing remote computer data capture are organised by repressive penal law[16] and State security law.[17]
- Capture of sounds and images in a private place. Procedures allowing remote capture, using a dedicated technical device, of words spoken in a private place or confidentially and of images in a private place, are organised by repressive law[18] and State security law.[19]
- Traffic and connection data. Several procedures allow the access to or the interception of a limited list of this kind of data under particular conditions:
  - Access to traffic and connection data retained by certain service providers is organised by repressive penal law[20] and State security law.[21] Additionally, access to this data may take place for the purposes of the prevention of attacks on public authorities' and on a restrictive list of operators' automated data processing systems, at the initiative of authorised and sworn agents from the national authority for information systems' security (ANSSI),[22] and for the purpose of the prosecution of one particular infringement to the Intellectual Property Code (fifth-class offence)[23] at the initiative of the independent public authority HADOPI.[24]

---

[14] Art. L. 851-1 ISC.

[15] Prior to the enactment of the laws that frame interception powers, the possibility for both intelligence services and law enforcement to collect electronic identifiers including passwords from service providers was criticised, for the precise reason that such data could in practice enable these services to intercept correspondence without outside any legal authorisation. On this topic see Estelle De Marco, "La captation des données" (Data capture), in Katarzyna Blay-Grabarczyk and Laure Milano (dir.), *Lutte contre le terrorisme et droits fondamentaux* (The combat against terrorism facing fundamental rights), Institut Universitaire Varenne, coll. "Colloques et Essais", L.G.D.J. – Lextenso, 3rd trim. 2017, pp. 91–107, p. 95; Estelle De Marco, *L'anonymat sur Internet et le droit*, Ph. D. thesis, Montpellier 1, 2005, ANRT (ISBN: 978-2-7295-6899-3; Ref.: 05MON10067), n° 850.

[16] Arts. 706-102-1 to 706-102-9 PPC, created by Law n° 2011-267 of 14 March 2011 and modified in 2014, 2015 and lastly by Law n° 2016-731 of 3 June 2016.

[17] Arts. L. 853-2 and L. 853-3 ISC, created by Law n° 2015-912 of 24 July 2015 and modified by Law n° 2017-1510 of 30 October 2017.

[18] Arts. 706-96 to 706-102 PPC, created by Law n° 2004-204 of 9 March 2004, lastly modified by Law n° 2016-731 of 3 June 2016.

[19] Arts. L. 853-1 and L. 853-3 ISC.

[20] Arts. L. 34-1 PECC; arts. 60-1, 60-2, 77-1-1, 77-1-2, 99-3 and 99-4 PPC.

[21] Arts. L. 851-1 ISC, created by Law n° 2015-912 of 24 July 2015.

[22] Arts. L. 34-1 PECC; art. L. 2321-3 Code of Defence modified by Law n° 2018-607 of 13 July 2018.

[23] This infringement is provided for in art. L. 336-3 of the Intellectual Property Code (IPC) and concerns a failure to meet the obligation of ensuring that one's own computer access to the Internet is not used for counterfeiting. It might amount (where some addition-

- Real-time collection of this data on service providers' networks is organised for the prevention of terrorist acts only, by State security law.[25]
- Direct collection of some of this data (including location data) by means of an intrusion into the computer system is organised by State security law[26] and by repressive penal law.[27]
- Preservation of and access to the content of the information accessed by users, through a request made to the relevant electronic communication operator, is organised by penal repressive law.[28]
- Real-time geolocation of a person, a vehicle or an object, is organised by repressive penal law[29] and State security law.[30]
- Detection of events likely to affect the security of public authorities' and of some listed operators' information systems, on operators' networks or on Internet access or hosting providers' information systems, may be implemented in certain cases by the National authority for information systems' security (ANSSI), under the Code of Defence.[31]

- Other forms of private communications, as well as public communications, are not subject to specific intercept or access procedures. They may be collected within the framework of the application of the ordinary legal system governing search and seizure of information held by a third party, organised by repressive penal law.
- Finally, all communications may be monitored at the service provider level for the purposes of real-time detection of "connections that may reveal a terrorist threat," as permitted by State security law, for the prevention of terrorism only.[32]

---

al circumstances are established) to a fifth-class (penal) offence punishable by fine (provided for in art. R. 335-5 IPC).

[24] Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (High Authority for the diffusion of works and the protection of rights on the Internet), provided for in art. L. 331-12 IPC. Its access to traffic data is provided for in art. L. 34-1, III PECC and art. L. 331-21 IPC.

[25] Art. L. 851-2 ISC, created by Law n° 2015-912 of 24 July 2015 and modified by Law n° 2017-1510 of 30 October 2017.

[26] Art. L. 851-6 ISC created by Law n° 2015-912 of 24 July 2015.

[27] Arts. 706-95-4 to 706-95-10 PPC created by Law n° 2016-731 of 3 June 2016.

[28] Arts. 60-2, 77-1-2, and 99-4 PPC.

[29] Art. 230-32 PPC.

[30] Arts. L. 851-5 and L. 853-3 ISC created by Law n° 2015-912 of 24 July 2015.

[31] Art. L. 2321-2-1 DC, created by Law n° 2018-607 of 13 July 2018.

[32] Art. L. 851-3 ISC created by Law n° 2015-912 of 24 July 2015.

2. Powers for the interception of electronic communications

Powers for the interception of electronic communications are different depending on the legal regime.

a) Law of penal procedure

In the law of penal procedure, five different legal regimes govern electronic communications intercept.

Firstly, electronic correspondence and other communication data may be intercepted in a certain number of situations at the initiative of certain judges (the investigating judge or the liberty and custody judge), following the procedure described in articles 100 to 100-8 and article 706-95 PPC.

Secondly, some other data intercept procedures, listed below, may be authorised for a more limited list of infringements at the initiative of the same judges:

- Access to stored electronic correspondences by means of an electronic identifier, provided for by articles 706-95-1 to 706-95-3.
- Intercept of technical connection data enabling the identification of terminal equipment or its user's subscription number, as well as of data related to the location of the terminal equipment used, by using an appropriate apparatus or technical device, provided for in articles 706-95-4 and 5 PPC.
- Intercept of correspondences sent or received by a terminal equipment by means of the same device or apparatus, under the same articles 706-95-4 and 706-95-5. In this situation, articles 100-4 to 100-7 PPC mentioned above are applicable. Capture of remote computer data, provided for in articles 706-102-1 to 706-102-9 PPC.
- Capture of spoken words in a private place or under confidentiality and images in a private place, using a dedicated technical device, provided for in articles 706-96 to 706-102 PPC.

Thirdly, another data capture procedure, namely real-time geolocation of a person, a vehicle or an object, without the consent of this person or the owner of this vehicle or object, may be ordered in more situations by the investigating judge or the district prosecutor (depending on the nature of the investigation) under articles 230-32 to 230-44 PPC.

Fourthly, two other data capture procedures might be ordered any investigation by certain judges or the district prosecutor (depending on the nature of the investigation):

- The requisition (even by electronic means) of traffic and connection data retained by access and hosting service providers,[33] provided for in articles 77-1-1 and 77-1-2 (preliminary investigation), 60-1 and 60-2 (flagrancy investigation) and 99-3 and 99-4 (judicial investigation, which means investigation procedure conducted by an investigative judge) PPC.

The order to preserve and to enable access to the content of the information accessed by users of electronic communication services, as provided for in articles 77-1-2 (preliminary investigation), 60-2 (flagrancy investigation) and 99-4 (judicial investigation) PPC.

Finally, the ordinary legal system governing search and seizure of information held by a third party may also enable the gathering of electronic communication data. It is set out in articles 76 to 76-3 (preliminary investigation), 56 to 59 (flagrancy investigation), 92 to 99-4 (investigation procedure conducted by an investigative judge). Search and seizure outside of the normal visiting hours may also be authorised by certain judges for the needs of a limited list of penal infringements, as provided for in article 706-89 PPC.

b) Law of intelligence agencies

Electronic correspondence and other communication data may be intercepted in a certain number of situations at the initiative of an important, if limited, list of agents, following the procedures described in the Internal Security Code.

aa) Areas in question

The following provisions may be used within the framework of the search for information by intelligence services and agents of several ministries listed by law and their implementing administrative acts, in the pursuit of a limited number of objectives.

Until October 2015 these objectives were:[34] national security; safeguard of essentials elements of the French scientific and economic potential; prevention of terrorism; prevention of organised crime and organised delinquency; prevention of the reconstitution or of the preservation of disbanded groups.[35]

---

[33] On the basis of art. L. 34-1 PECC and of art. 6 of the Law n° 2004-575 of 21 June 2004 regarding confidence in the digital economy (called "LCEN").

[34] Former art. L. 241-2 ISC.

[35] Art. L. 212-1 ISC lists exhaustively the categories of groups that must be disbanded by decree issued by the Council of Ministers (such as groups provoking armed events in the streets).

These objectives have been replaced by the search for information relating to the defence and promotion of the following "fundamental interests of the nation:"[36]

1. national independence, territorial integrity, and national defence;
2. major interests of foreign policy, implementation of France's European and international commitments, and prevention of any form of foreign interference;
3. major economic, industrial, and scientific interests of France;
4. prevention of terrorism;
5. prevention of:
   – attacks against the republican form of French institutions,
   – actions pursuing the reconstitution or the preservation of disbanded groups,[37]
   – collective violence likely to cause serious harm to public peace;
6. prevention of organised crime and delinquency;
7. prevention of proliferation of weapons for mass destruction.

Theoretically, the aforementioned objectives are the only ones that can justify the exercise of the exceptional measures described in the next subsection. However, a French legal provision and a Court of Cassation decision both give rise to the possibility of using the information gathered within the framework of these powers in order to feed the investigation into any penal infringement.

Indeed, the French Internal Security Code and Penal procedure Code require that any (other) crime or misdemeanour discovered upon exercising these special powers is brought to the attention of the district prosecutor (who has the discretion to take action on it), accompanied by related information.[38]

In addition, the French Court of Cassation decided, in a decision of 9 January 2018,[39] that a Judicial Police officer, acting under articles 53 to 67 PPC that regulates flagrancy investigations, has the duty to ensure the preservation of evidence that will likely disappear and of all that can be used to ascertain the truth, and that this duty may justify the access of this police officer to data collected within another framework, including under administrative law (in this case the data in issue was surveillance images collected upon authorisation of the prefect on the basis of the Internal Security Code). As a result, the access of justice to data collected for State

---

[36] According to the new art. L. 811-3 ISC, created by Law n° 2015-912 of 24 July 2015 of 26 July 2015.

[37] Art. L. 212-1 ISC. See footnote n° 35 above.

[38] Former art. L. 242-8 ISC (relating to correspondence intercepts) and current (from the 3 Oct. 2015) art. L. 811-2 of the latter Code (relating to all the measures described in the next subsection). These articles refer to art. 40 PPC, which in turn lays down this obligation.

[39] Court of Cassation, criminal chamber, 9 January 2018, n° 17-82.946, available at https://www.dalloz-avocats.fr/documentation/Document?id=CASS_LIEUVIDE_2018-01-09_1782946

security reasons, within the framework of penal investigations and at the initiative of judicial investigators, is not excluded.

bb) Legal provisions

Correspondence and other communication data intercepts cover different situations described and framed in the Internal Security Code.

(1) General framework

Before October 2015, the possibility of intercepting electronic communications for State security purposes was limited to the interception of electronic correspondence (former articles L. 241-1 *et seq.* ISC) and to the access to traffic and connection data retained by service providers (former articles L. 246-1 to L. 246-4 ISC). These powers of interception have been modified by Law n° 2015-912 of 24 July 2015 relating to intelligence (which entered into force on 3 October 2015),[40] which has also created other interception powers in terms of means and content. This law has been further modified or supplemented by a number of other legal acts in 2015,[41] 2016,[42] 2017[43] and 2018.[44]

Current powers of intercept are described in title V of Book VIII ISC (articles L. 851-1 to L. 855-1).

These powers are framed by titles I to title III of Book VIII ISC. In particular, interception techniques can only take place in principle upon prior authorisation of the Prime minister, delivered after obtaining the (non-binding) opinion of the national commission for the supervision of intelligence techniques, which is itself regulated in Title III. The form and the content of the request for authorisation, expressed by one of the competent ministries (Defence, Justice, Interior or Economy and Customs), as well as those of the authorisation and of the guarantees that must surround the implementation of the power, are regulated in Title II (articles L. 821-1 to L. 822-4).

However globally, the situations in which electronic correspondence and other communication data intercept may take place are wider, persons who may access

---

[40] Law n° 2015-912 of 24 July 2015 relating to intelligence.

[41] Law n° 2015-1556 of 30 November 2015, JORF n° 0278 of 1 December 2015, p. 22185, text n° 1.

[42] Law n° 2016-731 of 3 June 2016, JORF n° 0129 of 4 June 2016, text n° 1; Law n° 2016-987 of 21 July 2016, JORF n° 0169 of 22 July 2016, text n° 2

[43] Law n° 2017-55 of 20 January 2017, JORF n°0018 of 21 January 2017, text n° 2; Law n° 2017-258 of 28 February 2017, JORF n° 0051 of 1st March 2017, text n°3; Law n° 2017-1510 of 30 October 2017, JORF n° 0255 of 31 October 2017, text n° 1; Decree n° 2017-1095 of 14 June 2017, JORF n° 0139 of 15 June 2017, text n° 1.

[44] Law n° 2018-607 of 13 July 2018, JORF n° 0161 of 14 July 2018, text n° 1.

these correspondence and data are more numerous, accessed data is itself potentially more expansive, and safeguards in place are lower than those that are authorised within the framework of judicial intercept for the purpose of the repression of penal infringements.

(2) Powers of interception

Electronic correspondence transmitted by means of electronic communications may be intercepted under article L. 852-1, I ISC. The interception can be extended beyond the concerned person, to the persons belonging to the environment of the latter where there are reasons to believe that these persons are likely to provide information connected with the purpose that justified the authorisation.

Electronic correspondence sent or received by terminal equipment may also be intercepted directly by means of a technical device or apparatus, in order to pursue certain purposes only,[45] under article L. 852-1, II ISC.

Electronic correspondence transmitted within an electronic communication network using exclusively over-the-air transmission and not involving any electronic communication operator, may be intercepted in situations where this network is conceived to be domestically used by one person or a closed group of users, under article L. 852-2 ISC.Traffic and connection data[46] retained by service providers[47]

---

[45] Mentioned in 1°, 4° and 5° of art. L. 811-3 ISC. See above, Section I.A.2.b.aa.

[46] More precisely, data that may be accessed is more widely identified by law (in art. L. 851-1, former art. L. 246-1) as being "*information or documents processed or stored* by (ISP's) networks or electronic communications services, including technical information relating to the identification of subscription or connection numbers to electronic communications services, to the census of all subscription numbers and connection numbers of a specified person, to the geolocation of terminal equipment used, and to a user's communications regarding the list of called and calling numbers, the duration and date of communications." The decree of application of the original provision (art. L. 246-1, created by Law n°2013-1168 of 18 Dec. 2013, art. 20), specified that this data is only that which is of a technical nature only and cannot relate to the content of communications that can be accessed by the judiciary for the repression of crimes (Decree n°2014-1576 of 24 Dec. 2014 – http://www.legifrance.gouv.fr/eli/decret/2014/12/24/PRMD1422750D/jo). The decree of application of the new law (Decree n° 2016-67 of 29 January 2016) refers to the same data. It provides for an additional list of data that may be accessed by intelligence services or other Ministries, but only within the framework of administrative correspondence intercepts. It should be noted that the French Constitutional Council has recalled that traffic data that can be accessed for intelligence purposes cannot be related to the content of correspondence or to consulted information (Decision n°2015-713 DC, recital n° 55, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc2015713dc.pdf – press release: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/communique-de-presse.144139.html).

[47] This data is retained on the basis of art. L. 34-1 PECC (relating to electronic communications operators and access providers) and of art. 6 of the Law n°2004-575 of 21 June 2004 regarding confidence in the digital economy, so-called LCEN (relating to access and hosting providers).

can be accessed according to articles L. 851-1 and L. 851-2 of the new ISC. Such access may be obtained from these providers, or, solely for the purpose of terrorism prevention, through "real-time transmission," concerning persons previously identified as being "likely to be linked to a threat," and persons belonging to the latter's environment where serious reasons suggest that they are likely to provide information linked to the purpose that justifies the authorisation of the measure.

Direct collection of some of this data (connection data of a technical nature enabling the identification of terminal equipment or the identification of the subscription number of its user, as well as location data of terminal equipment) by means of an intrusion into the computer system is organised by article L. 851-6 ISC.

Real-time geolocation of a person, a vehicle or an object, without the consent of the person or the owner of the vehicle or object, is provided for in articles L. 851-5 and L. 853-3 ISC.

In addition, technical data relating to the location of terminal equipments may be collected "by network solicitation" and transmitted "in real time" by electronic communication operators to a department of the Prime Minister, under article L. 851-4 ISC.

Computer data, as it is stored or as they are displayed on the screen of the user or typed or received or sent, may be captured remotely where intelligence cannot be collected by another legal means, under articles L. 853-2 and L. 853-3 ISC.

Words spoken in a private place or under confidentiality and images in a private place may be captured, where intelligence cannot be collected by another legal mean, using a dedicated technical device, under articles L. 853-1 and L. 853-3 ISC.

International electronic communications, which means communications that are sent or received from abroad, may also be intercepted and are exclusively regulated by articles L. 854-1 to L. 854-9 ISC, whatever they are related to correspondence or connection data.

Finally, all communications may be monitored at the service provider level, for the needs of the prevention of terrorist acts only, in order to detect "connections that may reveal a terrorist threat" under article L. 851-3 ISC.

c) Prevention of attacks on automated data processing systems

For the security needs of public authorities' and of some listed operators' information systems (vitally important facilities or systems that are vital to the proper functioning of economy or society), some limited traffic data, namely the identity, the postal address and the electronic address of users or owners of vulnerable, threatened or attacked information systems, retained by electronic communications

operators,[48] can be requisitioned by authorised and sworn agents from the national authority for information systems' security (ANSSI), according to article L. 2321-3 of the Code of Defence,[49] in order to alert these persons to the vulnerability or the compromise of their system.

In addition, where the ANSSI is informed of a threat likely to affect the information system security of public authorities' or of some listed operators, this authority may implement, on operators' networks or on Internet access or hosting providers' information systems, devices that use technical markers in order to detect, as sole purpose, events that are likely to affect the security of the public authorities' or listed operators' information systems (article L. 2321-2-1 Code of Defence).[50]

d) Prevention of terrorist acts

All the measures described in the subsection relating to the law of intelligence agencies are also applicable for the prevention of terrorist acts.

However, as explained in this same subsection, only two of these measures can be implemented for the sole purpose of the prevention of terrorist acts:

- The possibility to implement an automated process on service providers' networks aimed at detecting "connections that may reveal a terrorist threat," under article L. 851-3 ISC.
- The possibility to request from service providers real-time transmission of traffic and connection data relating to a person previously identified as being "likely to be linked to a threat," and relating to persons belonging to the latter's environment where serious reasons suggest that they are likely to provide information linked to the purpose that justifies the authorisation of the measure, under article L. 851-2 ISC.

e) Customs Investigation Service

According to article 28-1 PPC, some specially nominated customs agents may be authorised to conduct judicial investigations in order to look for and report on a limited list of infringements, including infringements to the customs Code, by order of the district prosecutor or by rogatory commission issued by the investigating judge. Within that framework, judicial procedures described in subsection a) above may be applicable.

---

48 On the basis of art. L. 34-1 PECC.

49 Modified by Law n° 2018-607 of 13 July 2018.

50 Created by Law n° 2018-607 of 13 July 2018.

In addition, Decree n° 2015-1185 of 28 September 2015,[51] adopted in order to apply Law n° 2015-912, includes the National Directorate for Custom Intelligence and Investigations *(Direction nationale du renseignement et des enquêtes douanières)* in the list of specialised intelligence services that are entitled to exercise the powers described in subsection b) above.[52] This Directorate is an agency with national authority, within the General Directorate for customs and indirect rights, which itself rests within the Ministry of Public Action and Accounts.[53]

Moreover, according to article L. 811-4 ISC, a decree issued by the Council of State designates services other than intelligence services that may be authorised to exercise the powers granted to intelligence services as they are detailed in subsection b) above, which may include customs services (in addition to the Ministry of Justice and the Ministry of Economy and Budget). Decrees already issued under this provision,[54] codified in articles R. 811-2 and R. 851-1 to R. 851-4 ISC, have thus far only designated services belonging to the Ministry of Defence, the Ministry of the Interior, and the Ministry of Justice. However, subsequent decrees might follow.[55]

3. Responsibility for the technical performance of interception measures

Under French law, the technical enforcement of interception and data collection measures follows certain rules which differ depending on the nature of the procedure:

a) Interceptions and data collection performed under repressive penal law

Provisions that regulate interception and data collection performed under repressive penal law provide generally for a technical performance by the judge who ordered the measure or an appointed police officer. However, from 2016, most interceptions must be performed through a national platform for judicial interception, as a special rule that applies in the absence of technical impossibility.

---

[51] Decree n° 2015-1185 of 28 September 2015 (portant désignation des services spécialisés de renseignement), JORF n° 0225 of 29 September 2015 p. 17344, text n°1.

[52] Art. R. 811-1 ISC, modified by Decree n° 2016-1337 of 7 October 2016 and Decree n° 2017-1095 of 14 June 2017.

[53] http://www.douane.gouv.fr/articles/a12574-la-direction-nationale-du-renseignement-et-des-enquetes-douanieres.

[54] Décree n° 2015-1639 of 11 December 2015; Decree n° 2016-67 of 29 January 2016; Decree n° 2017-36 of 16 January 2017; and Decree n° 2018-543 of 29 June 2018.

[55] Before the entry into force of Law n° 2015-912 of 24 July 2015 – therefore before 3 October 2015 – agents of the Ministry for Economy, therefore possibly customs agents, could access traffic and connection data if individually appointed and duly authorised, for limited purposes listed in former art. 241-2 ISC (former art. 246-1 ISC created by art. 20 of Law n° 2013-1168 of 18 December 2013). Correspondence intercept could also be authorised on the proposal of the Ministry in charge of customs (former art. L. 242-1 ISC).

aa) Technical performance according to provisions that regulate interceptions

The installation of a correspondence interception system, as well as the use of an electronic identifier in order to access stored correspondence are performed by the magistrate who ordered the measure or by a police officer, who may in turn require any qualified agent belonging to a service or organisation placed under the authority of the Ministry in charge of electronic communications, or from any qualified agent belonging to an authorised electronic communications service provider.[56]

The installation of an apparatus or technical device in order to remotely capture (1) technical connection data that enables the identification of terminal equipment or its user's subscription number, as well as data related to the location of the terminal equipment used, (2) correspondences sent or received by this terminal equipment, (3) the geolocation of a person, a vehicle or an object, and (4) spoken words in a private place or under confidentiality or images in a private place, are performed by the magistrate who ordered the measure or by a police officer, who may in turn require any qualified agent belonging to a service, a unit or a body placed under the authority of the Ministry of the Interior, the list of which is established by decree. In the above-mentioned hypotheses 3 and 4, the police officer may alternatively require a police agent to perform the installation.[57]

The installation of a technical device that enables remote computer data capture is performed by the magistrate who ordered the measure or by a police officer, who may in turn require a police agent or any qualified agent belonging to a service, a unit or a body placed under the authority of the Ministry of the Interior or the Ministry of Defence, and which list is established by decree, to perform the installation of the technical devices that enable data captures authorised by law.[58]

The preservation of the content of the information accessed by users is performed by the personnel of the relevant electronic communication operator on request from a police officer, and the information is provided by electronic or telematic means.[59]

Search and seizures are performed by the the district prosecutor or a police officer, who may call upon any qualified person.[60] When the procedure is directed by an investigating judge, search and seizures are performed by this judge or the police officer appointed by this judge.[61]

---

[56] Respectively arts. 100-3 and 706-95 PPC and art. 706-95-3, §2 PPC.

[57] Respectively arts. 706-95-1, 706-95-2 and 706-95-8 PPC, 230-32 and 230-36 PPC, and 706-96-1, 706-96-2 and 706-99 PPC.

[58] Arts. 706-102-1, 706-102-2, and 706-102-6 PPC.

[59] Arts. 60-2, 77-1-2 and 99-4 PPC.

[60] Arts. 60 (flagrancy investigation), 77-1 (preliminary investigation) PPC.

[61] Art. 97 PPC.

bb) Technical performance through the national platform for judicial interceptions

From 2016, article 230-45 PPC[62] states that unless it is technically impossible, certain interception measures must be transmitted through a national platform for judicial interceptions,[63] which organises the centralisation of their execution. This platform is placed under the authority of the Ministry of Justice.[64] The types of communications interception measures concerned are (1) correspondence interception,[65] (2) requests for preservation of and access to the content of the information accessed by users of electronic communication services, (3) requests for traffic and connection data addressed to operators by electronic or telematic means, and (4) geolocation of a person, a vehicle or an object.

In addition, a decree adopted in the Council of State must provide for the modalities under which data and correspondence captured under articles 706-95-4 and 706-95-5 PPC (capture of technical connection data that enables the identification of a terminal equipment or its user's subscription number, as well as data relating to the location of the terminal equipment used, and correspondences sent or received by this terminal equipment) must be centralised and stored in the national platform for judicial interceptions, unless technical impossibility prevents this.

b) Interceptions and data collection performed under State security law

The Internal Security Code states that intelligence gathering techniques (which are applicable in relation to the prevention of terrorism, organised crime and organised delinquency)are implemented under the authority[66] (and under authorisation)[67] of the Prime Minister after consultation of the National Commission for the Control of Intelligence Techniques.[68] The Prime Minister organises traceability of the execution of authorised techniques and sets out the basis for centralising collected information.[69]

---

[62] Created by Law n° 2016-731 of 3 June 2016, Art. 88, JORF n° 0129 of 4 June 2016. Art. 230-45 has been later modified by Law n° 2017-258 of 28 February 2017 (art. 35) and Law n° 2018-699 of 3 August 2018 (art. 16).

[63] Regulated, according to art. 230-45 PPC, by decree, which has been codified in arts. R. 40-42 to R. 40-56 PPC.

[64] Art. R. 40-42 PPC.

[65] Arts. 100 to 100-7, art. 706-95, art. 74-2, art. 80-4, and art. 709-1-3 PPC.

[66] Art. L. 822-1 ISC.

[67] Art. L. 821-1 ISC.

[68] Art. L. 822-1 ISC.

[69] Art. L. 822-1 ISC.

In principle, intelligence gathering techniques can only be implemented by individually appointed and regulated agents.[70] Two different procedures govern information gathering, depending on whether the relevant electronic communication operator is asked to provide its assistance:

– Electronic correspondence intercepts,[71] administrative access to traffic and connection data,[72] administrative direct access to traffic and connection data using "network solicitation" and "real-time transmission by operators,"[73] as well as, concerning the prevention of terrorism only, real-time collection of traffic and connection data[74] and monitoring of service providers' networks in order to detect "connections that may reveal a terrorist threat,"[75] can only be technically performed following the procedure described in article L. 871-6 ISC,[76] according to which these measures can only be technically performed by qualified agents[77] belonging to the organisation or the service provider in whose premises and installations the measure must be implemented.

– Real-time geolocation of a person, a vehicle or an object, without the consent of the person or the owner of the vehicle or object,[78] remote computer data capture;[79] remote words and image capture[80] and remote capture of location and connection data using a technical device[81] can only be performed:

---

[70] This results from a general provision (art. L. 821 ISC), repeated in some specific ones implying an intrusion into a system or a private place in order to organise remote data capture (arts. L. 851-6, II and 853-1 ISC).

[71] Art. L. 852-1 ISC.

[72] Art. L. 851-1 ISC.

[73] Art. L. 851-4 ISC.

[74] Relating to a person previously identified as presenting a threat on service providers' networks, art. L. 851-2 ISC.

[75] Art. L. 851-3 ISC.

[76] Created by art. 11 of Law n° 2015-912 of 24 July 2015. This procedure takes over the provisions of the former art. L. 242-9 ISC, which was relating to correspondences intercept only. The only element that changes, beyond the fact that the procedure is extended to more numerous measures, is that the technical performance of these measures can only be performed by order of the Prime Minister, whereas such an order was the duty of the Ministry for Electronic Communications in former art. L. 242-9.

[77] This provision does not specify that agents must be "individually appointed and regulated," as required by the general principle established in art. L. 821-1 ISC. However, this principle is supposed to be enforced by the Prime Minister. In addition, the obligation of electronic communication operators to respect the secrecy of correspondence (art. L. 32-3 PECC) and of electronic communication data (L. 34-1, II PECC), and more generally their obligation to respect personal data (General Data Protection Regulation (EU) n° 2016/679) imply the individual appointment and regulation of all agents who accesses private information (without which the enforcement and supervision of these obligations could not be ensured).

[78] Art. L. 851-5 ISC.

[79] Art. L. 853-2 ISC.

[80] Art. L. 853-1 ISC.

[81] Art. L. 851-6 ISC.

– where the implementation of the technical device does not require intrusion into a private place, by individually appointed and regulated agents,[82] particularly in the case of remote capture of location and connection data;[83]

– where the implementation of the technical device does require intrusion into a private place, by individually appointed and regulated agents who belong to one of the services that may be authorised to use intelligence gathering techniques, the list of which being established by decree issued by the Council of State.[84]

4. Legitimacy of data transfers between security and law enforcement agencies

Services in charge of the repression of criminal offences and services in charge of State security are theoretically separated. However, several of these services fall within the responsibility of the same direction or ministry. In addition, some services in charge of the repression of crime also have some crime prevention duties, which fall into the scope of application of intelligence gathering techniques. Finally, a certain exchange of information is organised on both sides.

a) Separation of functions

The repressive function and the intelligence function are separated. However, some services exercising the former and some services exercising the latter come under the control of the same ministry (Ministry of the Interior), and even the same body (an example being the National Gendarmerie[85]) or directorate (an example being the General Directorate for Internal Security, which is both a security intelligence service and a specialised judicial police service).[86]

In addition, some services in charge of crime repression are given some missions of crime prevention, which fall into the scope of application of intelligence gathering techniques. This is the case, for example, under the authority of the General Director of the National Police, with the sub-directorate in charge of the combat against organised crime and financial delinquency, and with the subdirectorate in charge of the combat against cybercrime.[87]

---

[82] Art. L. 821-1 ISC; art. L. 851-6 ISC.

[83] Art. L. 851-6 ISC.

[84] Art. L. 853-3, § 2 ISC.

[85] Art. L. 421-1 ISC.

[86] Art. R. 811-1 ISC; Decree n° 2014-445 of 30 April 2014, art. 1, JORF n° 0102 of 2 May 2014, text n° 23. See also https://www.interieur.gouv.fr/Le-ministere/DGSI/Mission-de-police-judiciaire-specialisee

[87] Art. R. 851-1 ISC.

Moreover, it may be noted that some administrative measures are very close to other measures that fall under the power of the judicial police, targeting similar behaviours, without offering the same guarantees against arbitrariness, which leads legal authors to evoke problematic situations of "confusion between the administrative and the judicial phase."[88]

Regarding the supervision of powers, most[89] communications intercepts as defined above are performed under the control of an independent judge within the framework of crime repression, whereas they are performed under the control of an independent administrative authority – which however presents less guarantees against arbitrariness than the judicial authority – within the framework of intelligence gathering.

b) Exchange of data between law enforcement authorities and intelligence agencies

Several provisions provide for the possibility of exchanging information between law enforcement authorities and intelligence agencies.

aa) Passing on of data by law enforcement authorities to intelligence agencies

The Internal Security Code provides for the possibility, in certain circumstances, for listed intelligence services or subservices to access certain judicial data processing. Some agents from intelligence services may access[90] data processing containing information collected during judicial investigations related to a series of infringements including attacks against persons, goods, or public tranquillity.[91] Several purposes authorise such access, including response missions that are likely to present risks for public order,[92] the pursuit of a series of objectives including non-exhaustively[93] the preservation of national independence or the combat against terrorist acts,[94] and administrative inquiries before recruitment or accreditation.[95]

---

[88] Laure Milano, Les implications sur les droits de la défense (Implications on the rights of the defence), in *Lutte contre le terrorisme et droits fondamentaux (The combat against terrorism facing fundamental rights)*, Institut Universitaire Varenne, coll. "Colloques et Essais", L.G.D.J. – Lextenso, 3rd trim. 2017, pp. 131–147, quot. p. 134.

[89] The others are performed under the supervision of the public or district prosecutor, which in France is not independent from the executive power.

[90] This possibility is provided for in arts. L. 234-1 to L. 234-4, R. 234-1 to R. 234-3 ISC.

[91] These judicial data processing are provided for in art. 230-6 PPC.

[92] Art. L. 234-3 ISC.

[93] The complete list of concerned objectives consists of purposes n°1, 4 and 5 listed in art. L. 811-3 ISC, mentioned in details below in Section I.A.2.b.aa.: National independence, territorial integrity, and national defence; prevention of terrorism; prevention of (a) attacks against the republican form of French institutions, (b) actions pursuing the

In addition, individually appointed and duly accredited agents of intelligence services and of specialised services of the Gendarmerie and the Police may all access, for the needs of the prevention and repression of attacks to national fundamental interests and terrorist acts, personal data processing established for other purposes. These are listed in article L. 222-1 ISC and include the national vehicle registration file, the national driving license file, the system for managing identity cards, the system for managing passports, the foreign national dossiers management system, and the digital prints and photographs of foreign nationals who are not nationals of a Member State of the European Union, collected in two situations (where they have been controlled at a frontier post and they do not meet the conditions for entry into the French territory, and where they apply for a visa to stay in France or in a State which is party to the Schengen Convention, at a consulate or at the external border of a State which is party to this Convention).[96]

bb) Passing on of data by intelligence agencies to law enforcement authorities

French law authorises – and even obliges – intelligence services to provide the judiciary, in certain cases, with information resulting from intelligence investigations, while the Court of Cassation seems to admit that judicial police officers are authorised to access administrative files for the needs of the investigation they are in charge of.

Indeed, according to article 40 PPC, when an established authority, a public officer or a public servant learns, during the performance of their duties, of a crime or of a misdemeanour, they must give notice of it to the district prosecutor, and must provide this magistrate with any information, official records and other investigative acts relating to this crime or misdemeanour. The district prosecutor evaluates what further action should be taken in accordance with article 40-1 PPC.

This principle also appears in article L. 811-2 ISC, which mentions schematically that the procedure surrounding the exercise of the powers of the intelligence services is without prejudice of the provisions of article 40 PPC.

In addition, the French Court of Cassation decided in a decision of 9 January 2018[97] that a Judicial Police officer, acting under articles 53 to 67 PPC that regulates flagrancy investigations, has the duty to ensure the preservation of evidence that will likely disappear and of all that can be used to ascertain the truth, and that

---

reconstitution or the preservation of disbanded groups, and (c) collective violence likely to cause serious harm to public peace.

94 Art. L. 234-4 ISC.

95 Arts. L. 114-1, L. 234-1, L. 234-2, R. 234-1 and R. 234-2 ISC.

96 Arts. L. 222-1 and R. 222-1.

97 Court of Cassation, crim. ch., 9 January 2018, n° 17-82.946 https://www.dalloz-avocats.fr/documentation/Document?id=CASS_LIEUVIDE_2018-01-09_1782946.

this duty may justify the access of this police officer to data collected within other frameworks, including under administrative law (the documents in issue in this case were surveillance images collected upon authorisation of the prefect on the basis of the Internal Security Code). As a result, the access of justice to data collected for State security reasons, within the framework of penal investigations and at the initiative of judicial investigators, is not excluded.

Finally and more specifically, article L. 2312-4 Code of Defence enables French courts, within the framework of a proceeding, to request the declassification and the communication of information protected by national defence confidentiality, from the administrative authority in charge of classification (which must immediately bring the matter to the attention of the Commission for national Defence Confidentiality).

cc) Exchange of data with competent authorities in other countries

One provision of the Internal Security Code regulates the exchange of data with competent authorities in other countries. In Chapter V dedicated to international cooperation in the area of access to personal data automated processing, article L. 235-1, §1 states that "the data included in personal data automated processing managed by the national Police and the national Gendarmerie services may be transmitted, within the framework of international agreements duly introduced into the French legal order, to international cooperation organisations in the field of judicial police or to foreign services, which ensure a sufficient level of protection of private life, of freedoms and of fundamental rights of persons with regard to the processing or possible processing of these data. The sufficient nature of the protection level that is ensured by a given State is assessed based on, *inter alia*, the applicable legal provisions in this State, the security measures that are applied in that State, the processing specific characteristics such as its purposes and its length, as well as the nature, the source and the destination of processed data."

Article L. 235-1, §2 goes on to clarify that "the national Police and Gendarmerie services may receive data contained in data processing managed by international cooperation organisations in the field of judicial police or by foreign services, within the framework of international agreements" referred to in the previous paragraph.

It may be noted that this exchange of information escapes independent supervision.

– Information provided by foreign services or international organisations cannot be requested from the Prime Minister by the national commission in charge of the supervision of intelligence gathering techniques, as an exception to its power to request "all information needed to accomplish its tasks."[98]

[98] Art. L. 833-2, §4 ISC.

– "Exchanges with foreign services or with international organism that are competent in the area of intelligence" cannot be concerned by a request for communication addressed to the Prime Minister by the "parliamentary delegation for intelligence" established by Law n° 2013-1168 of 18 December 2013 in order to exercise a parliamentary supervision of the government's action in the area of intelligence.[99]

B. Statistics on Electronic Communications Interception

Statistics are produced at the level of the national platform for judicial intercept, in relation to communications intercepts performed by the judiciary for the repression of crime and delinquency, and by the National Commission for the Control of Security Interceptions in relation to intelligence gathering techniques. Beyond the missions of these structures, there is no obligation, under French law, to produce statistics relating to judicial or intelligence intercept activity.

1. Communication intercepts for the purpose of judicial penal repression

Regarding communications intercepts performed by the judiciary for the repression of crime and delinquency, few statistics were published until 2017. For example, it was reported in various publications for the year of 2012, that 35,000 telephone communications intercepts, 650,000 judicial requisitions of traffic data and 12,000 geolocations measures were performed.[100]

By a press release of 3 November 2017,[101] the Ministry of Justice announced that, at the level of the platform for judicial intercept (PNIJ), which is being evolving and improved,

– 8500 judicial intercepts were ongoing (4500 in July 2017),
– 2 million requests for gaining access to fata were answered annually,
– 600,000 communications were intercepted each week,
– 900,000 text messages were intercepted each week.

---

[99] Art. 12 of the law, which modifies Ordonnance n°58-1100 of 17 November 1958 relating to the functioning of parliamentary assemblies.

[100] *Franck Johannès*, "Les écoutes judiciaires ont explosé depuis 2006," 18 March 2014, Le Monde, http://www.lemonde.fr/societe/article/2014/03/18/les-ecoutes-judiciaires-ont-explose-depuis-2006_4384910_3224.html. Some publications evoked the number of 20,000 instead of 35,000 communication intercepts, see http://www.senat.fr/leg/ppr13-422.html. Some media evoked in addition 5,500,000 "additional services" such as access to detailed invoicing: see *Franck Johannès*, above [last accessed on 19 Dec. 2018].

[101] Ministry of Justice, Press release, "La plate-forme nationale des interceptions judiciaires en chiffres" 3 November 2017, available at http://www.presse.justice.gouv.fr/archives-communiques-10095/communiques-de-2017-12858/la-plateforme-nationale-des-interceptions-judiciaires-en-chiffres-30997.html.

The press release clarified that more than 90 % of ancillary measures (such as itemised bills, number identification, geolocation) were provided by the PNIJ, which also enables the intercept of G4 communications, which was "impossible beforehand."

It has to be noted, however, that the efficiency and the cost of this platform, which is still not fully operational, are regularly criticised,[102] by judicial investigators themselves who evoke system faults that impede investigations.[103]

2. Communication intercept for intelligence purposes

Before the entry into force of Law n° 2015-912, communication intercepts performed under intelligence law were subject to an annual report of the National Commission for the Control of Security Interceptions (*Commission nationale de contrôle des interceptions de sécurité*, CNCIS).

This Commission has been replaced in the new law by the National Commission for the Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement*, CNCTR), which also publishes a report annually.

In its report for 2017, the CNCTR announced that during the period covering 2016 and 2017, it delivered 70,432 prior opinions related to requests for the implementation of an intelligence-gathering technique, as broken down in the following figures (at the exclusion of requests relating to international electronic communication surveillance).[104]

---

[102] See, e.g., Marc Rees, 25 January 2018, "Interceptions: troisième report pour la PNIJ," Next Inpact, https://www.nextinpact.com/news/106027-interceptions-troisieme-report-pour-pnij.htm; Jean-Marc Manach, "Pour vous écouter, l'État dépensera au moins 385 millions d'euros (et probablement bien plus)," 17 March 2018, Slate.fr, http://www.slate.fr/story/159046/pnij-ecoutes-judiciaires-ministere-justice-retard-facture-385-millions-euros.

[103] Jean-Marc Leclerc, "La police dénonce les bugs à répétition des écoutes judiciaires," 10 May 2018, Le Figaro, http://www.lefigaro.fr/actualite-france/2018/05/10/01016-20180510ARTFIG00155-la-police-denonce-les-bugs-a-repetition-des-ecoutes-judiciaires.php?redirect_premium; Pierre Alonso, "Avec la Pnij, les écoutes téléphoniques en plein vertige", 10 November 2017, Liberation, https://www.liberation.fr/france/2017/11/10/avec-la-pnij-les-ecoutes-telephoniques-en-plein-vertige_1609380; Etienne Combier, "Ecoutes judiciaires: le ministère de la Justice sur la défensive", 30 October 2017, Les Echos, https://www.lesechos.fr/30/10/2017/lesechos.fr/030805866292_ecoutes-judiciaires---le-ministere-de-la-justice-sur-la-defensive.htm; Alain Acco, "Un syndicat police dénonce les ratés de la plateforme d'écoutes judiciaires", 26 September 2017, Europe 1, https://www.europe1.fr/societe/un-syndicat-police-denonce-les-rates-de-la-plateforme-decoutes-judiciaires-3446201; Syndicat des Cadres de la Sécurité Intérieure, "PNIJ : un ratage annoncé, mais qui persiste !", 26 September 2017, https://www.scsi-pn.fr/archives/3751

[104] Commission nationale de contrôle des techniques de renseignement, 2ème rapport d'activité 2017, available at https://www.cnctr.fr/_downloads/NP_CNCTR_2018_rapport_annuel_2017.pdf, pp. 45–46.

	2016	2017	Evolution
Access to connection data in non-real time (subscribers identification or subscription number census – art. 851-1 ISC)	32,096	30,116	-6.2%
Access to connection data in non-real time (other requests, including of itemised bills – art. 851-1 ISC)	15,021	18,512	+23.2%
Real-time geolocation (art. 851-4 ISC)	2,426	3,751	+54.6%
Correspondence intercept (art. L. 852-1 ISC)	8,137	8,758*	+7.6%
Other intelligence-gathering techniques	9,408	9,295	-1.2%
All intelligence-gathering techniques	67,088	70,432	+5%

*: amongst which 34 % were initial requests and 66 % were requests for extension.[105] The CNCTR also announced that in 2017 it had given 786 unfavourable opinions (outside the requests for non-real-time access to connection data), corresponding to 3.6 % of the total of opinions rendered. This rate is lower than in 2016 (6.9 %), which is due, according to the Commission, to a better quality of requests, especially concerning proportionality.[106] The CNCTR moreover clarifies that the Prime Minister did not grant a single authorisation following an unfavourable opinion.[107]

II. Principles of Electronic Communications Interception in Constitutional and Criminal Procedural Law

Constitutional principles frame the powers of the State in terms of interception and collection of electronic communications, which is reflected in the PPC.

A. Constitutional Safeguards of Electronic Communication

Constitutional safeguards of electronic communications include the principle of proportionality and benefit to both electronic communications and personal data.

1. Areas of constitutional protection

French constitutional safeguards do exist but do not refer explicitly to the protection of electronic communications.

---

105 *Ibid.*, p. 48.

106 *Ibid.*, p. 49.

107 *Ibid.*

The right to respect for private and family life is protected by the French Constitutional Council under article 2[108] (in addition to, sometimes, article 4[109]) of the French Human and Citizens Rights Declaration of 1789,[110] the latter Declaration being included in the so-called French "constitutionality bloc" (which has a constitutional value). The French Constitutional Council may also protect some aspects of the right to respect for private life under the principle of personal freedom[111] and more specifically individual freedom, the guardian of which is the judicial authority under article 66 of the Constitution[112] (in addition to the Parliament which must set up the rules, more widely, relating to fundamental guarantees granted to citizens for the exercise of public freedoms, under article 34 of the Constitution[113]).

---

[108] French Constitutional Council, Decision n° 2016-590 QPC of 21 October 2016 2015, recital n° 3. Art. 2 of the French Human and Citizens Rights Declaration of 1789 states: "The aim of every political association is the preservation of the natural and imprescriptible rights of Man. These rights are Liberty, Property, Safety and Resistance to Oppression". The Declaration is available in English on the Constitutional Council website: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/cst2.pdf

[109] French Constitutional Council, Decision n° 2004-492 DC of 2 March 2004, J.O. 10 March 2004, p. 4637, recital n° 4; Decision n° 2005-532 DC of 19 January 2006, recital n° 9. Art. 4 of the French Human and Citizens Rights Declaration of 1789 states: "Liberty consists in being able to do anything that does not harm others: thus, the exercise of the natural rights of every man has no bounds other than those that ensure to the other members of society the enjoyment of these same rights. These bounds may be determined only by Law."

[110] See, e.g., French Constitutional Council, Decision n° 2004-492 DC of 2 March 2004, J.O. 10 March 2004, p. 4637, recital n° 4; Decision n° 2005-532 DC of 19 January 2006, recital n° 9.

[111] Other elements of personal freedom are, under French law, the freedom of movement, the right to not being arbitrarily arrested or sequestered, the right to be judged with all legal guarantees and the principle of inviolability of the home. See Jacques Robert/Jean Duffar, *Droits de l'homme et libertés fondamentales*, 7th ed., 1999, p. 27; art. 136 PPC; Estelle De Marco, "Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux," 4 June 2009, Juriscom.net, p. 3, available at http://www.juriscom.net/uni/visu.php?ID=1133

[112] The French Constitution is available in English on the Constitutional Council website: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/constitution_anglais_juillet2008.pdf. See also Constitutional Council, Decision n° 2004-492 DC of 2 March 2004, Recital n°4.

[113] The Constitutional Council considers that the refusal to take into consideration the right to respect of private life can be liable to hurt personal freedom: Decision n° 94-352 DC, 18 Jan. 1995, J.O. 21 Jan. 1995, p. 1154 and JCP 1995, II, 22 525, note *Frédérique Lafay*. The Council also analysed the implementation of technical mechanisms allowing picking-up, fixing or registering words or images without the consent of interested people, in the light of personal freedom: Decision n° 2004-492 DC, 2 March 2004, JORF 10 March 2004, p. 4637. The Council also extends the notion to some personal data filing systems: Decision n° 2004-492 DC, 2 March 2004, JORF 10 March 2004, p. 4637, § n° 64. Such protection of private life under art. 66 of the Constitution that guarantees individual freedom has been seen as a way to prevent the administrative judge being seized in relation to private life violations, which could also explain why the Constitutional Council now mostly base the protection of private life on art. 2 of the French Human and Citizens

The notion of private life does not have a precise definition in the constitutional jurisprudence, and is not mentioned in the French Constitution, having been deducted by the Constitutional Council from the above-mentioned provisions of the Human and Citizens Rights Declaration of 1789. It is not clear whether rights that are traditionally considered as being covered by the right to private life, such as the protection of the home and the protection of correspondence,[114] are protected by the Constitutional Council as private life elements or as stand-alone rights, under the same articles 2 and 4 of the Human and Citizens Rights Declaration of 1789. However, on the basis of these provisions, the Constitutional Council protects the secrecy of electronic communications, personal data, the secrecy of computer data, and confidential words and images.

a) Secrecy of electronic communications

The secret of correspondence transmitted by means of electronic communications is protected under articles 2 and 4 of the French Human and Citizens Rights Declaration of 1789.[115] Also protected under the same constitutional basis are transmissions via terrestrial frequencies,[116] information consulted using an electronic communications network[117] and connection and traffic technical data,[118] including terminal equipment location data and identifiers, and users' subscription numbers.[119]

Rights Declaration of 1789, which is not an area reserved to the judicial judge only: see Vincent Mazeaud, "La constitutionnalisation du droit au respect de la vie privée" (the constitutionalisation of the right to respect for private life), nouveaux cahiers du Conseil constitutionnel n°48 (dossier vie privée), June 2015, pp. 7–20, especially §§6 and 8, also available at https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-constitutionnalisation-du-droit-au-respect-de-la-vie-privee

[114] According to the doctrine, private life is a notion that encompasses sub-rights which are at least the protection of the home or the secret of correspondence, as well as the "freedom" of private life and to correspond (since freedom is a requirement that enables a person to organise the secrecy of his or her activities and behaviours): see, e.g., Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT, n° 132 *et seq.*; Virginie Peltier, *Le secret des correspondances*, PU d'Aix-Marseille, 1999, pp. 99 *et seq.*, n°119 *et seq.*; Pierre Kayser, *La protection de la vie privée par le droit*, 3rd ed., 1995, especially pp. 11–12, p. 60. See also Vincent Mazeaud, "La constitutionnalisation du droit au respect de la vie privée"; *op. cit*., §7 (in relation to the freedom of action) and §11 (in relation to privacy as a "strain notion" in the Constitutional Council jurisprudence).

[115] See Constitutional Council, Decision n° 2004-492 DC of 2 March 2004, recital n° 4; Decision n° 2016-590 QPC of 21 October 2016 2015, recital n° 6.

[116] Constitutional Council, Decision n° 2016-590 QPC of 21 October 2016, recital n° 9.

[117] See, e.g., Constitutional Council, Decision n°2015-478 QPC of 24 July 2015, recitals n° 10 *et seq.*

[118] Constitutional Council, Decision n°2005-532 DC of 19 January 2006, recitals n° 9 to 21.

[119] Constitutional Council, Decision n° 2015-713 DC of 23 July 2015, recitals n° 27 to 29. Location data relating to a person or a vehicle are also included in the protection.

b) Personal data protection

In addition, the protection of private and family life covers,[120] according to the Constitutional Council, the right to the protection of personal data, and more precisely "collection, recording, retention, consultation and communication of personal data."[121]

c) Secrecy of computer data

More widely, the Constitutional Council considers that article 2 of the Human and Citizens Rights Declaration of 1789 protects data from computing systems, regardless of its nature.[122]

The seizure of a computing system or of terminal equipment is also protected, not as a privacy element but under the right to property, which is, according to the Constitutional Council, conferred by articles 2 and 17 of the Human and Citizens Rights Declaration of 1789.[123] As a result, the copying of such data, within the framework of a search and seizure procedure, cannot be executed without an authorisation from a judicial[124] or administrative[125] judge.

d) Intercept of confidential words and images

Although the interception of confidential words and images in a private and even in a public place is not strictly speaking an electronic communications interception, the demarcation between both might be small since intercepted words might be confidentially exchanged with a remote partner through an electronic transmission of voice, and captured images might be images seen by the person under surveillance through a computer system, or even images of the behaviour of this same person during an electronic call, which can be a source of information concerning their state of mind within the framework of the call.

---

120 This opinion is discussed amongst legal authors, some of them considering that private life and the personal data sphere do not overlap. On this debate see Estelle De Marco, *Comparative study between Directive 95/46/EC and the GDPR including their relations to fundamental rights*, March 2018, Deliverable D2.10, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/, Section 2.2.2.

121 Constitutional Council, Decision n° 2012-652 DC of 22 March 2012, recital n° 8; Decision n° 2013-681 DC of 5 December 2013, recital n° 27; see also Constitutional Council, Commentary on the Decision n° 2014-690 DC of 13 March 2014, p. 20.

122 See, e.g., Constitutional Council, Decision n° 2016-536 QPC of 19 February 2016, recital n° 14; Decision n° 2016-600 QPC of 2 December 2016, Recital n° 13.

123 Constitutional Council, Decision n° 2016-600 QPC of 2 December 2016, recital n° 17.

124 Constitutional Council, Decision n° 2016-536 QPC of 19 February 2016, recital n° 14.

125 Constitutional Council, Decision n° 2016-600 QPC of 2 December 2016, recital n° 13.

The Constitutional Council considers that the Constitution (including the Human and Citizens Rights Declaration of 1789) also protects data in the form of images captured and transmitted through video-surveillance systems installed in public places[126] and building entrances,[127] as well as images captured in private places and registered private or confidential words.[128]

2. Proportionality of access to data

According to the French Constitutional Council, limitations to the right to private and family life and to the secrecy of electronic communications and personal data "must be justified by a reason in the public interest and implemented properly and in a manner proportionate to this end."[129] In other decisions, in relation to the preservation of the freedom of expression, the Council used a slightly different test that any limitation to this right must be necessary, adequate and proportionate to the aim pursued.[130]

Overall, the meaning of these formulas is close to the notions of "necessity" and "proportionality" used by the European Court of Human Rights (ECtHR).[131] Indeed, in the words of one author, the French Constitutional Council seems to have "aligned its jurisprudence with the one of the ECtHR, since it performs a similar

---

[126] Constitutional Council, Decision n° 94-352 DC of 18 January 1995, recitals n° 3 and 4.

[127] Constitutional Council, Decision n° 2010-604 DC of 25 February 2010, recitals n° 19 to 20.

[128] Constitutional Council, Decision n° 2015-713 DC of 23 July 2015, recitals n° 69 to 74.

[129] Constitutional Council, Decision n° 2012-652 DC of 22 March 2012, recital n° 8; Decision n° 2013-681 DC of 5 Dec. 2013, recital n° 27; see also Constitutional Council, Commentary on the Decision n°2014-690 DC of 13 March 2014, p. 20, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2014690DCccc_690dc.pdf [last accessed on 18 Sept. 2015].

[130] See, e.g., Constitutional Council, Decision 2009-580 DC of 10 June 2009, recital n° 15; Decision n° 2012-647 DC of 28 February 2012, recital n° 5; Decision n° 2010-3 QPC of 28 May 2010, recital n° 6.

[131] The European Convention on Human Rights (ECHR) is in France of infra-constitutional but supra-legal force, even though the national law is subsequent to the Convention. Indeed, the Convention is directly integrated into the local system by the Constitution, as its art. 55 states that "Treaties or agreements duly ratified or approved shall, upon publication, prevail over Acts of Parliament, subject, with respect to each agreement or treaty, to its application by the other party" (the second part of the text does not receive application because the principle of reciprocity does not apply as regards the ECHR.). See Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux," in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, p. 39, n° 68; Estelle De Marco and Cormac Callanan, in C. Callanan, M. Gercke, E. De Marco and H. Dries-Ziekenheiner, *Internet blocking – balancing cybercrime responses in democratic societies*, October 2009, n° 6.5.2.2, available at http://www.aconite.com/blocking/study (French version available at http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/) [last accessed on 18 Sept. 2015].

proportionality test, between general interests on the one hand and the limitation brought to a freedom on the other hand, based on the principle of separation of powers."[132] Moreover, since 2004, the Constitutional Council refers sometimes directly to the European Convention on Human Rights in its decisions.[133]

The Constitutional Council may verify the adequacy of the measure in relation to its aim,[134] the appropriateness of the resources allocated in pursuit of this aim (even though the Council considers that it is not its duty to verify whether the aim could have been achieved using other means),[135] and the necessity to combat the issue that justifies the measure[136] (which are three elements that compose the notion of "necessity" according to the ECtHR).[137]

Regarding proportionality in the strictest sense, and particularly in the area of the protection of the right to private life,[138] the French Constitutional Council recalls

---

[132] Olivier Dutheillet de Lamothe, "L'influence de la Cour européenne des droits de l'Homme sur le Conseil constitutionnel," 13 Feb. 2009, Conseil constitutionnel, visite du Président et d'une délégation de la Cour européenne des droits de l'homme au Conseil constitutionnel, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/pdf/Conseil/cedh_130209_odutheillet.pdf, p. 9. See also Estelle De Marco, *Analyse du nouveau mécanisme de prevention de la contrefaçon à la lumière des droits et libertés fondamentaux*, 4 June 2009, p. 16, Juriscom.net, http://juriscom.net/2009/06/hadopi-analyse-du-nouveau-mecanisme-de-prevention-de-la-contrefacon-a-la-lumiere-des-droits-et-libertes-fondamentaux/

[133] Constitutional Council, Decision n° 2004-505 DC of 19 November 2004, https://www.conseil-constitutionnel.fr/decision/2004/2004505DC.htm; see Joël Andriantsimbazovina, "Ouverture : l'extériorisation de la prise en compte de la Convention européenne des droits de l'homme", in "La prise en compte de la Convention européenne des droits de l'homme par le Conseil constitutionnel, continuité ou évolution ?", Cahiers du Conseil constitutionnel n° 18 (Dossier: Constitution et Europe) – July 2005, https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-prise-en-compte-de-la-convention-europeenne-des-droits-de-l-homme-par-le-conseil-constitutionnel.

[134] See, e.g., Constitutional Council, Decision n° 2009-599 DC of 29 Dec. 2009, recital n° 81; see also Valérie Goesel-Le Bihan, "Le contrôle de proportionalité exercé par le Conseil constitutionnel, technique de protection des libertés publiques?" http://juspoliticum.com/Le-controle-de-proportionnalite.html [last accessed on 22 Sept. 2015].

[135] See, e.g., Constitutional Council, Decision n° 2000-433 DC of 27 July 2000, recital n° 41; see also Valérie Goesel-Le Bihan, "Le contrôle de proportionalité exercé par le Conseil constitutionnel, technique de protection des libertés publiques?", *op. cit*.

[136] See, e.g., Constitutional Council, Decision n° 2009-580 DC of 10 June 2009, recital n° 13.

[137] See, e.g., Estelle De Marco, *Comparative study between Directive 95/46/EC and the GDPR including their relations to fundamental rights*, March 2018, Deliverable D2.10, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/, Section 2.3.2.3; Estelle De Marco (ed.), *Identification and analysis of the legal and ethical framework*, July 2017, Deliverable D2.2, MANDOLA EU project, GA n° JUST/2014/RRAC/AG/ HATE/6652, http://mandola-project.eu/publications/, Section 4.1.3.2, 3.

[138] In this area, the proportionality principle is supposed to include, in the light of the ECtHR jurisprudence, the strict minimisation of the measure and the provision for safeguards. See, e.g., Estelle De Marco, *Comparative study between Directive 95/46/EC and*

that it is the mission of the Parliament, on the basis of article 34 Constitution, to lay down the rules relating to fundamental safeguards that must be granted to individuals for the exercise of their public freedoms.[139] In addition, the Constitutional Council generally verifies whether legal guarantees are adequate and sufficient.[140]

Among these legal guarantees or safeguards lies the respect for the principle that offences and penalties must be defined by law. Other safeguards are the respect of the rights of the defence;[141] the limitation of the duration of the measure;[142] the limitation of the number of people who may suffer from the limitation;[143] the limitation and the definition of the purposes[144] and of the situations[145] in which the measure can be exercised; and the existence of an independent control of the implementation of the measure.[146] During these controls, the nature and sensitivity of data that may be collected are naturally also taken into account.[147]

The protection of fundamental rights, and particularly the proportionality of access to data, is therefore theoretically ensured at the Constitutional Council level. However, some legal authors highlight a supervision that might be too theoretical in certain circumstances, "overshadowing some practical realities,"[148] which leads to the non-censorship of laws that might have disproportionate practical effects.

---

the GDPR including their relations to fundamental rights, March 2018, *op. cit.*, Section 2.3.2.4.

139 See, e.g., Constitutional Council, Decision n° 2009-580 DC of 10 June 2009, recital n° 23, *op. cit*.

140 See, e.g., Constitutional Council, Decision n° 2013-681 DC of 5 December 2013, recital n° 28; Constitutional Council, Decision n° 2012-652 DC of 22 March 2012, recital n° 8; see also *La proportionnalité dans la jurisprudence constitutionnelle*, 5ème conférence des Chefs d'institution de l'Association des Cours constitutionnelles ayant en partage l'usage du français, 8–13 July 2008, p. 7, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/Bilan_2008/confV_accpuf_libreville_juillet2008.pdf

141 See, e.g., Constitutional Council, Decision n° 2009-580 DC of 10 June 2009, recital n° 14, *op. cit*.

142 See, e.g., Constitutional Council, Decision n° 2004-492 DC of 2 March 2004, recital n° 59; Decision n° 2013-681 DC of 5 Dec. 2013, recital n° 28.

143 See, e.g., Constitutional Council, Decision n° 2004-492 DC of 2 March 2004, recital n° 59, *op. cit.*; Decision n° 2012-652 of 22 March 2012, recital n° 10.

144 See, e.g., Constitutional Council, Decision n° 2012-652 of 22 March 2012, recital n° 10 *op. cit*.

145 See, e.g., Constitutional Council, Decision n° 2004-492 DC of 2 March 2004, recital n° 59, *op. cit.*; Decision n° 2013-681 DC of 5 December 2013, recital n° 28.

146 See, e.g., Constitutional Council, Decision n° 2004-492 DC of 2 March 2004, recital n° 59, *op. cit.*

147 See, e.g., Constitutional Council, Decision n° 2012-652 of 22 March 2012, recitals n° 10 and n° 11, *op. cit*.

148 Olivier Cahn, "Un Etat de droit, apparemment …" (A State under the rule of law, apparently …), Actualité Juridique, Penal, April 2016, n°4, p.201-204, quoted by Emmanuel Daoud, "Le point de vue d'un avocat" (The point of view of an advocate), in Katarzyna

3. Consequences for the interception of electronic communication

The primary consequence of the Constitutional Council jurisprudence is that the law authorising the limitation of the right to private life must be necessary and proportionate, which implies *inter alia* that it provides for adequate safeguards. Otherwise, the Constitutional Council may declare the law unconstitutional, if the law is referred to it before it is enacted. The request must for this purpose be submitted by the President of the Republic, the Prime Minister, the President of one of the two Parliament chambers, or by 60 members of the National Assembly or 60 members of the Senate.[149]

In addition, after the law is enacted, citizens can challenge the compliance of a law with the Constitution through a trial. The judge must in this case, if the request is considered admissible and if criteria established by law are met,[150] transmit the request to the Court of Cassation or to the Council of State (depending on the nature of the trial), which may transfer the request in turn to the Constitutional Council.[151]

This being said, and despite this supervision mechanism, the penal procedure surrounding electronic communication interception appears to suffer from a lack of necessity and proportionality in certain respects (even though this lack is less serious than that found in relation to interceptions for intelligence purposes).[152]

One of the major concerns is related to the duty to minimise interferences in citizens' private life, which should call for reducing the potential use of the power to the minimum necessary, whereas article 40 PPC and the other provisions that take over its substance enable – and worse, command – any public agent to report to the district prosecutor any crime or misdemeanour discovered upon exercising his or her powers, along with related information. The district prosecutor has the discretion to take action on it, and several provisions clarify that if the data capture measure reveals penal infringements other than those that motivated the measure, this is not a cause for nullity of subsequent proceedings.[153] This issue is even intensified

---

Blay-Grabarczyk and Laure Milano (dir.), "Lutte contre le terrorisme et droits fondamentaux" (The combat against terrorism facing fundamental rights), Institut Universitaire Varenne, coll. "Colloques et Essais, " L.G.D.J. – Lextenso, 3rd trim. 2017, pp. 171–183, quot. p. 182.

149 Art. 61 Constitution.

150 These criteria are set out in the organic Law n° 2009-1523 of 10 December 2009.

151 Art. 61-1 Constitution. See also "Comment saisir le Conseil constitutionel?," http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/le-conseil-constitutionnel/la-saisine/comment-saisir-le-conseil-constitutionnel-/comment-saisir-le-conseil-constitutionnel.17421.html

152 Estelle De Marco, "La captation des données" (Data capture), in Katarzyna Blay-Grabarczyk and Laure Milano (dir.), "Lutte contre le terrorisme et droits fondamentaux" (The combat against terrorism facing fundamental rights), Institut Universitaire Varenne, coll. "Colloques et Essais," L.G.D.J. – Lextenso, 3rd trim. 2017, pp. 91–107.

153 See, e.g., art. 230-37 relating to geolocation. On this issue see, e.g., Laure Milano, "Les implications sur les droits de la défense" (Implications on the rights of the defence),

by the possibility for the judiciary to access certain data collected by the administration within the framework of intelligence activities[154] (of which the use should itself be restricted to the purpose for which they were collected).

Other weaknesses in terms of necessity and proportionality cover the lack of independence of the district prosecutor whose powers are increasing,[155] the possibility of accessing stored correspondence outside the guarantees that govern correspondence interception,[156] an increasing transfer of competences from the judiciary to intelligence-gathering services[157] and a relative protection, in practice, of persons whose function is crucial in a State governed by the rule of law, including advocates.[158]

4. Statutory protection of privacy and personal data

In addition to the constitutional protection, all private life aspects are protected by the French civil judge on the basis of article 9 of the Civil Code (CC) and of article 8 of the European Convention on Human Rights (ECHR).[159] Moreover, some other legal provisions protect specific private life aspects, including personal or confidential data, such as the following:

– Correspondence (including electronic correspondence) is protected during transmission by articles 226-15 and 432-9 PC.[160]

---

in *Lutte contre le terrorisme et droits fondamentaux* (The combat against terrorism facing fundamental rights), Institut Universitaire Varenne, coll. "Colloques et Essais," L.G.D.J. – Lextenso, 3rd trim. 2017, pp. 131–147, p. 139.

154 See above, Section I.A.4.b.cc.

155 Laure Milano, "Les implications sur les droits de la défense" (Implications on the rights of the defence), *op. cit.*, p. 147.

156 See below, Section III.B.2.b.bb.; see Estelle De Marco, "La captation des données," *op. cit*.

157 Emmanuel Daoud, "Le point de vue d'un avocat" (The point of view of an advocate), in Katarzyna Blay-Grabarczyk and Laure Milano (dir.), "Lutte contre le terrorisme et droits fondamentaux" (The combat against terrorism facing fundamental rights), Institut Universitaire Varenne, coll. "Colloques et Essais," L.G.D.J. – Lextenso, 3rd trim. 2017, pp. 171–183, p. 178.

158 See below, Section III.B.3.

159 See, e.g., a case of annulment of a criminal procedural act consisting of the geolocation of the accused, because French law did not provide for a clear legal basis authorising such a procedural act and providing for adequate safeguards: Cass. crim., 22 October 2013, n°13-81945.

160 Art. 226-15 PC: "Maliciously opening, destroying, delaying or diverting of correspondence sent to a third party, whether or not it arrives at its destination, or fraudulently gaining knowledge of it, is punished by one year's imprisonment and a fine of €45,000." "The same penalty applies to the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by electronic means, or the setting up of a device designed to produce such interceptions." Art. 432-9: "Except where provided for by law, the ordering, committing or facilitation of the misappropriation, suppression or opening of correspondence, and the disclosure of the contents of such correspondence, by a

- The protection of personal data is organised by Law n° 78-17 of 6 January 1978 (most recently modified in 2018 in order to include changes due to the entry into force of the General Data Protection Regulation). Some of its provisions are subject to penal charges according to articles 226-16 to 226-24 PC. The principle of specified, explicit, and legitimate purpose is declared in article 6 of Law n° 78-17 modified.
- Attacks on automated data processing systems are punished by articles 323-1 to 323-8 PC, last modified in 2015.[161]

Finally and more widely, non-private secrecies are also protected, primarily professional secrecy,[162] but the Penal Procedure Code generally states that these secrets cannot be opposed without legitimate ground to judicial investigators,[163] outside privileged correspondence.[164]

B. Powers in the Penal Procedure Code

As a result of constitutional principles, powers in the law of criminal procedure must be clearly defined by specific provisions.

1. Requirement of (reasonable) clarity for powers in the law of criminal procedure

As has been mentioned in A. above, the definition of coercive powers in criminal procedural law must be described by the law itself, and the principle "no crime without legal definition" is applicable under French law, meaning *inter alia* that criminal statutes must be defined precisely by the legislator before the commission of a criminal act can be assumed.

---

person holding public authority or discharging a public service mission acting in the course of or on the occasion of his office or duty, is punished by three years' imprisonment and a fine of €45,000.

The same penalties apply to the persons referred to under the previous paragraph, or to employees of electronic communication networks open to the public, or to employees of a supplier of telecommunication services, who, acting in the performing of their office, order, commit or facilitate, except where provided for by law, any interception or misappropriation of correspondence sent, transmitted or received by a means of telecommunication, or the use or the disclosure of its contents."

161 An English version of these provisions that does not take into account the most recent legal modifications is available at http://www.legifrance.gouv.fr/content/download/1957/13715/version/4/file/Code_33.pdf. Most modifications are relating to penalties, which have been increased.

162 Art. 226-13 PC.

163 E.g., art. 99-3 PPC.

164 See below, Section III.B.3.a.

2. Differentiation and classification of powers in the law of criminal procedure

As a consequence, coercive powers in French criminal procedural law must be and are based on differentiated, precise, and specific provisions.

III. Powers for Accessing Electronic Communication Data in the Law of Criminal Procedure

Powers of accessing electronic communications, understood in a broad sense, cover powers relating to the interception of content data, including sounds and visual images, and to the collection and retention of technical connection and traffic data.

A. Overview

As explained in subsections I.A.1. and 2., the above-mentioned powers are subject to several procedures precisely described in the Penal Procedure Code.

B. Interception of Content Data

It has already been noted that the French Penal Procedure Code distinguishes between correspondence and other kinds of electronic data and communications. Correspondence can be intercepted following specific procedures, whereas other procedures enable the interception of other type of communications and the access to stored correspondence (beyond the search and seizure procedure, which will be analysed later in this report).

These other procedures include procedures allowing remote data capture and a procedure that requires electronic communications operators to preserve the content of the information accessed by their users.

1. Statutory provision

a) Correspondence interceptions

The interception of the content of electronic correspondence is set out in articles 100 to 100-8[165] and articles 706-95 and 706-95-4 to 706-95-10 PPC.[166] In addi-

---

[165] An English translation of arts. 100 to 100-7, taking into account modifications of the law up to 2005, is found at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf (art. 100-5 was modified in 2010; arts. 100, 100-2 and 100-3 were modified by Law n° 2016-731 of 3 June 2016).

tion, some specific powers of intercept are established in articles 80-4 and 709-1-3 PPC.

Articles 100 to 100-7 PPC provide the investigating judge with the power to authorise the interception, recording and transcription of correspondence transmitted by means of electronic communication where the investigation of felonies and misdemeanours punishable by imprisonment of not less than two years calls for it. Article 80-4 extends this possibility to inquiry into the death or disappearance of a person.

Article 100-8 PPC regulates the interception of correspondence transmitted by means of electronic communication which targets an address of communication (e.g., an email address) used on the territory of a Member State of the European Union, whereas it does not take place within the framework of a European Investigation Order.

Article 709-1-3 extends the application of articles 100 to 100-8 PPC to situations where there are reasonable grounds to believe that, at the end of their incarceration, a sentenced person has not respected their obligation to refrain from contacting certain persons or frequenting certain places. In this case the measure is enforced on instruction of the judge responsible for the enforcement of sentences.

Finally, articles 706-95 and 706-95-4 to 706-95-10 PPC provide the liberty and custody judge with the interception powers of the investigating judge where the needs of a flagrancy inquiry or of a preliminary inquiry into a list of organised crime or delinquency offences call for it.

All these provisions may be found in the Appendix of the current report. Core provisions, which are articles 100 to 100-7 and article 706-95, are the following:

Article 100

For the investigation of felonies and misdemeanours, if the penalty incurred is equal to or in excess of two years' imprisonment, the investigating judge may order the interception, recording and transcription of correspondence transmitted by means of electronic communication where the requirements of the investigation call for it. Such operations are made under his authority and supervision.

The interception decision is made in writing. It is not a jurisdictional decision and cannot be appealed.

Article 100-1

The order made pursuant to article 100 must include all the details identifying the link to be intercepted, the offence which justifies resorting to an interception, and the duration of this interception.

---

[166] An English translation of these articles taking into account modifications of the law up to 2005 is found at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf (art. 706-95 was modified by a law of 2015 and afterward by an ordinance of December 2016; arts. 706-95-4 to 706-95-10 have been created by Law n° 2016-731 of 3 June 2016).

Article 100-2

This decision can last for a maximum duration of four months. It may be extended only by following the same conditions as to form and duration, without the total period of interception being longer than one year, or, if is concerned an infringement under articles 706-73 and 706-73-1, two years.

Article 100-3

The investigating judge or the judicial police officer appointed by him may require any qualified agent of a service or body placed under the authority or supervision of the Minister in charge of electronic communication, or any qualified agent of an authorised network operator or purveyor of electronic communication services to set up an interception device.

Article 100-4

The investigating judge or the judicial police officer appointed by him drafts an official record of both the interception and recording operations. This official record mentions the date and time when the operation started and ended.

The recordings are placed under closed official seals.

Article 100-5

The investigating judge or the judicial police officer appointed by him transcribes any correspondence which is useful for the discovery of the truth. An official record is made of these transcriptions. The transcription is attached to the case file.

Correspondence in a foreign language is transcribed into French with the assistance of an interpreter appointed for this purpose.

On penalty of nullity, no transcription may be made of any correspondence with an advocate relating to the exercise of the defendant's rights.

On penalty of nullity, no transcription may be made of any correspondence with a journalist allowing identifying a source in breach of article 2 of the Law of 29 July 1881 on Freedom of the Press.

Article 100-6

The recordings are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution.

An official record is made of the destruction.

Article 100-7

No interception may be made on the telephone line of a member of Parliament or senator unless the president of the assembly he belongs to is informed of the interception by the investigating judge.

No interception may be made on a telephone line connecting the chambers or domicile of an advocate unless the president of the bar association is informed of this by the investigating judge.

No interception may be made on a telephone line connecting the chambers or domicile of a judge or prosecutor unless the president or the prosecutor general of the court with jurisdiction over the area in question is informed of this by the investigating judge.

The formalities set out by the present article are prescribed under penalty of nullity.

Article 706-95

If the needs of a flagrancy inquiry or a preliminary inquiry into one of the offences within the scope of articles 706-73[167] and 706-73-1[168] justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor, authorise the interception, recording or transcription of correspondence by telecommunication, under the provisions of paragraph two of article 100, article 100-1 and articles 100-3 to 100-7, for a maximum period of one month, renewable once under the same conditions of form and duration. These operations are carried out under the supervision of the liberty and custody judge.

For the application of the provisions of articles 100-3 to 100-5, the powers conferred on the investigating judge or the judicial police officer nominated by him are exercised by the district prosecutor or the judicial police officer appointed by him.

The liberty and custody judge who has authorised this interception is immediately informed by the district prosecutor of any actions carried out in accordance with the previous paragraph, including official records drafted pursuant to his authorisation, by way of the application of articles 100-4 and 100-5.

b) Interception of correspondence sent or received by terminal equipment

The interception of electronic correspondence sent or received by terminal equipment is set out in articles 706-95-4 to 706-95-10 PPC.[169]

Article 706-95-4

I.-If the needs of an inquiry into one of the offences within the scope of articles 706-73 and 706-73-1 of the current Code justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor, authorise judicial police officers to use a technical device or apparatus mentioned in 1° of article 226-3 of the Penal Code[170]

---

[167] Art. 706-73 refers to 20 organised crime or delinquency offences such as murder, torture and acts of barbarity, and felonies and misdemeanours relating to drug trafficking. For extended details please see Appendix, Section B.2.

[168] Art. 706-73-1 refers to 11 organised crime or delinquency offences such as misdemeanour of fraud committed by an organised gang and misdemeanour of violation of personal data processing operated by the State committed by an organised gang. For extended details please see Appendix, Section B.2.

[169] An English translation of these articles taking into account modifications of the law up to 2005 is found at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf (art. 706-95 was modified by a law of 2015 and afterward by an ordinance of December 2016; arts. 706-95-4 to 706-95-10 have been created by Law n° 2016-731 of 3 June 2016).

[170] Art. 226-3 PC punishes by a prison term of 5 years and a fine of €300,000: (1) The manufacture, import, detention, exhibition, offer, rental or sale of apparatuses or of technical devices whose nature is such that they may enable to perform operations that constitute the offence set out under the second paragraph of article 226-15 PC or which, being designed for the detection of conversations from a distance, enable the commission of an offence under article 226-1 PC, or which purpose is to capture computer data under articles 706-102-1 and 706-102-2 of the Penal Procedure Code and L. 853-2 of the Internal Security Code and which are enumerated on a list drawn up pursuant to the conditions determined by decree of the Conseil d'Etat, where such acts are committed, including by negligence, in the absence of a ministerial authorisation whose conditions of granting are determined by that decree or if they are committed without respecting the conditions provided for in this authorisation; (2) The advertising of an apparatus or a technical device

in order to collect technical connection data (…).[171] The authorisation is delivered for a maximum period of one month, renewable once under the same conditions.

II.-The liberty and custody judge of the district court may also, under the same conditions, authorise the use of this device or apparatus in order to intercept correspondence sent or received by a terminal equipment. In this situation the procedures laid down in articles 100-4 to 100-7 of the current Code are applicable and the powers conferred to the investigating judge or to the judicial police officer appointed by him are exercised by the district prosecutor or to the judicial police officer appointed by this magistrate. The authorisation is delivered for a maximum period of forty-eight hours, renewable once under the same conditions.

III.-In case of emergency resulting from an imminent risk of evidence being damaged or an imminent risk of serious harm to persons or goods, the authorisation mentioned in the I and II may be delivered by the district prosecutor. It includes a statement on the factual circumstances that establish the existence of the imminent risk. The authorisation must then be confirmed by the liberty and custody judge within a maximal period of twenty four hours. Failing that, the operation is brought to an end, collected data or correspondence are placed under closed official seals and cannot be exploited or used in the proceedings.

The liberty and custody judge who delivered or confirmed the authorisation is informed without undue delay by the district prosecutor with regard to acts that have been performed under the current article and with regard to official records drawn-up pursuant to his authorisation.

Article 706-95-5

I.-If the needs of a judicial investigation into one of the offences within the scope of articles 706-73 and 706-73-1 of the current Code justify this, the investigating judge may, after obtaining the opinion of the district prosecutor, authorise judicial police officers to use a technical device or apparatus mentioned in 1° of article 226-3 of the Penal Code in order to collect technical connection data (…)[172]. The authorisation is delivered for a

---

liable to enable the commission of the offences set out under article 226-1 and the second paragraph of article 226-15, where this advertisement constitutes an incentive to commit such offences or the advertising of an apparatus or a technical device whose purpose is computer data capture under articles 706-102-1 and 706-102-2 of the Penal Procedure Code and L. 853-2 of the Internal Security Code where this advertisement constitutes an incentive to use it fraudulently.

Art. 226-1 punishes by a penalty of one year's imprisonment and a fine of €45,000 any wilful violation of the intimacy of the private life of other persons by resorting to any means of: 1° intercepting, recording or transmitting words uttered in confidential or private circumstances, without the consent of their speaker; 2° taking, recording or transmitting the picture of a person who is within a private place, without the consent of the person concerned. Where the offences referred to in the present article were performed in the sight and with the knowledge of the persons concerned without their objection, although they were in a position to do so, their consent is presumed;

Art. 226-15, §2 punishes by a prison term of 1 year and a fine of 45 000 € the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by electronic means, or the setting up of a device whose nature is such that it might enable to achieve such interceptions.

171 See below Section C.1. in relation to the content of this provision which provides for the collection of traffic and subscription data.

172 See below, Section C.1. in relation to the content of this provision which provides for the collection of traffic and subscription data.

maximum period of two months, renewable under the same conditions, without the total period of operations being longer than six months.

II.-The investigating judge may also, under the same conditions, authorise the use of this device or apparatus in order to intercept correspondence sent or received by a terminal equipment. In this situation the procedures laid down in articles 100-4 to 100-7 of the current Code are applicable. The authorisation is delivered for a maximum period of forty-eight hours, renewable once under the same conditions.

Article 706-95-6

Authorisations mentioned in articles 706-95-4 and 706-95-5 shall be the subject of a written order stating the reasons for the authorisation. This order does not constitute a jurisdictional decision and cannot be appealed.

Article 706-95-7

Operations mentioned in articles 706-95-4 and 706-95-5 are carried out under the authority and supervision of the magistrate who authorised them and cannot, under penalty of nullity, pursue another purpose than that of investigating and detecting penal infringements that are mentioned in the decision of this magistrate.

The fact that these operations reveal penal infringements other than those mentioned in the magistrate's decision that authorises these operations is not a cause for nullity of incidental proceedings.

Article 706-95-8

The district prosecutor, the investigating judge or the judicial police officer may require any qualified agent of a service, of a unit or of a body placed under the authority of the Ministry of the Interior, the list of which is set by decree, with a view to proceeding with the use of the technical device or apparat mentioned in articles 706-95-4 and 706-95-5.

Article 706-95-9

The judicial police officer draws-up an official record of operations carried out under the I of articles 706-95-4 and 706-95-5. This official record mentions the date and time at which each of the necessary operations started and at which these operations ended.

The judicial police officer attaches to the official record the collected data that are useful for ascertaining the truth

Article 706-95-10

Collected data pursuant to the I of articles 706-95-4 and 706-95-5 are destroyed, on the initiative of the district prosecutor or of the public prosecutor, at the date on which prosecution is barred under the statute of limitations or when a final decision has been given on the substance. An official record is made of the destruction.

Correspondences intercepted pursuant to II of articles 706-95-4 and 706-95-5 can only relate to the person or to the communication link referred to in the authorisation of interception operations.

c) Interception of stored correspondence

Since Law n°2016-731 of 3 June 2016, the interception of stored electronic correspondence is set out in articles 706-95-1 to 706-95-3 PPC:

Article 706-95-1

If the needs of an inquiry into one of the offences within the scope of articles 706-73 and 706-73-1 justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor, authorise, by way of reasoned order, access, remotely

and without the knowledge of the person concerned, to correspondence stored by means of electronic communication and accessible using an electronic identifier. Data to which access has been enabled can be seized and registered or copied on any support.

Article 706-95-2

If the needs of a judicial information into one of the offences within the scope of articles 706-73 and 706-73-1 justify this, the investigating judge may authorise, by way of reasoned order, access, remotely and without the knowledge of the person concerned, to correspondence stored by means of electronic communication and accessible using an electronic identifier. Data to which access has been enabled can be seized and registered or copied on any support.

Article 706-95-3

Operations mentioned in articles 706-95-1 and 706-95-2 are carried out under the authority and the supervision of the magistrate who authorised them and cannot, under penalty of nullity, pursue another purpose than that of investigating and detecting penal infringements that are mentioned in the decision of this magistrate.

The magistrate or the judicial police officer appointed by him may require any qualified agent of a service or body placed under the authority or supervision of the Minister in charge of electronic communication, or any qualified agent of an authorised network operator or purveyor of electronic communication services to set up the operations mentioned in articles 706-95-1 and 706-95-2.

The fact that these operations reveal penal infringements other than those mentioned in the magistrate's decision that authorises these operations is not a cause for nullity of incidental proceedings.

Where the electronic identifier is linked to the account of an advocate, of a magistrate, of a member of the Parliament or of a senator, article 100-7 is applicable.

d) Remote data capture

Remote data capture is set out in articles 706-102-1 to 706-102-9 PPC:[173]

Article 706-102-1

If the needs of an inquiry into one of the penal infringements within the scope of articles 706-73[174] and 706-73-1[175] justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor, authorise, by way of reasoned order, judicial police officers and agents that have been appointed by the district prosecutor, to implement a technical device aiming to access computer data, in all places and without the consent of the concerned people, and to register, store and transmit those data, as they are stored in the computer system, or as they are displayed on the screen of the user of the computer system, or as they are typed by the user of the system, or as they are received and sent by audio-visual devices.

The district prosecutor may appoint any entitled natural or legal person who is registered in one of the lists provided for in article 157, in order to perform the technical operations that allow the realisation of the technical device mentioned in the first paragraph of the current article. The district prosecutor may also prescribe the use of the State's means

---

[173] See note on English translation of these articles above. However, these articles have been modified by Law n°2016-731 of 3 June 2016.

[174] See Appendix, Section B.2.

[175] See Appendix, Section B.2.

that are covered by confidentiality for national defence purposes in accordance with the forms laid down by Chapter Ist of Title IV of Book Ist.

Article 706-102-2

If the needs of a judicial investigation into one of the penal infringements within the scope of articles 706-73[176] and 706-73-1[177] justify this, the investigating judge may, after having requested the opinion of the district prosecutor, authorise, by way of reasoned order, judicial police officers and agents that have been appointed by rogatory commission, to implement a technical device aiming to access computer data, in all places and without the consent of the concerned people, and to register, store and transmit those data, as they are stored in the computer system, or as they are displayed on the screen of the user of the computer system, or as they are typed by the user of the system, or as they are received and sent by audio-visual devices.

The investigating judge may appoint any entitled natural or legal person who is registered in one of the lists provided for in article 157, in order to perform the technical operations that allow the realisation of the technical device mentioned in the first paragraph of the current article. The investigating judge may also prescribe the use of the State's means that are covered by confidentiality for national defence purposes in accordance with the forms laid down by Chapter Ist of Title IV of Book Ist.

Article 706-102-3

Under penalty of nullity, the decision of the liberty and custody judge of the district court or of the investigating judge, taken pursuant to articles 706-102-1 and 706-102-2, mentions the penal infringement that justifies the operation, the exact location or the comprehensive description of the computer systems concerned and the duration of operations.

The authorisation decision taken pursuant to article 706-102-1 is delivered for a maximum duration of one month, renewable once under the same conditions. The authorisation decision taken pursuant to article 706-102-2 is delivered for a maximum duration of four months, renewable under the same conditions, without the total period of operations being longer than two years.

Article 706-102-4

The operations provided for in the current section are carried out under the authority and the supervision of the magistrate who authorised them, who may at all time order their interruption. Under penalty of nullity, these operations cannot pursue another purpose than that of investigating and detecting penal infringements that are mentioned in the decisions of this magistrate.

The fact that these operations reveal penal infringements other than those mentioned in these decisions is not a cause for nullity of incidental proceedings.

Article 706-102-5

In order to implement the technical device mentioned in articles 706-102-1 and 706-102-2, the liberty and custody judge of the district court, at the request of the district prosecutor, or the investigating judge, may authorise the introduction to a vehicle or to a private place, including outside the times mentioned in article 59 PPC,[178] without the knowledge or without the consent of the owner or of the possessor of the vehicle or of

---

[176] See Appendix, Section B.2.

[177] See Appendix, Section B.2.

[178] Art. 59 states that, except where they are requested from within a building or in the exceptional cases provided for by law, searches and house visits may not be undertaken before 6 am or after 9 pm.

the occupier or of any person having a right to this vehicle or place. If the device must be introduced in a home outside the times mentioned in article 59, this authorisation must be delivered by the liberty and custody judge of the district court, on the special request of the district prosecutor or by the investigating judge. These operations cannot pursue any other aim than implementing the technical device and are performed under the authority and supervision of the liberty and custody judge or of the investigating judge. The current paragraph is also applicable to operations aimed at uninstalling the technical device that has been implemented.

In order to implement the device mentioned in articles 706-102-1 and 706-102-2, the liberty and custody judge of the district court, at the request of the district prosecutor or the investigating judge may also authorise the transmission of this device by means of an electronic communications network. These operations are performed under the authority and supervision of the liberty and custody judge of the district court or of the investigating judge. The current paragraph is also applicable to operations aiming at uninstalling the technical device that has been implemented.

The technical device mentioned in article 706-102-1 can neither be implemented in a computer system located in places covered by articles 56-1,[179] 56-2,[180] 56-3[181] and 56-5,[182] nor in the vehicle, the business premises or the home of people mentioned in article 100-7.

Article 706-102-6

The investigating judge or the judicial police officer appointed by him or required by the district prosecutor may require any qualified agent of a service or unit or body placed under the authority or supervision of the Ministry of the Interior or of the Ministry of Defence, a list of which is determined by means of a Decree, in order to install the device mentioned in articles 706-102-1 and 706-102-2.

Article 706-102-7

The investigating judge or the judicial police officer appointed by him or required by the district prosecutor draws-up an official record of both the operations of installation of the device mentioned in articles 706-102-1 and 706-102-2, and the operations of computer data capture. This official record mentions the date and times when the operation started and the date and time when the operation ended.

The recordings of computer data are placed under closed official seals.

Article 706-102-8

The investigating judge or the judicial police officer appointed by him or required by the district prosecutor describes or transcribes, in an official record filed in the criminal case file, the data that are useful to ascertain the truth. No sequence relating to private life but that has no relation with penal infringements mentioned in the decisions that authorise the measure can be kept in the criminal case file.

Data in a foreign language are transcribed into French with the assistance of an interpreter appointed for this purpose.

---

[179] This article refers to business premises or the home of advocates.

[180] This article refers to business premises of media companies, audio-visual communication companies, online public communication companies, press agencies, to the professional vehicles of these companies, and to the homes of journalists where the investigation relates to their professional activities.

[181] This article refers to professional premises of doctors, notaries, or bailiffs.

[182] This article refers to seizures taking place at judicial premises and at the home of people exercising judicial office, and aiming at seizing documents likely to be covered by deliberation secrecy.

Article 706-102-9

The recordings of computer data are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution.

An official record is made of the destruction.

In addition, the Penal Procedure Code organises the remote capture of spoken words in a private place or under confidentiality and images in a private place (articles 706-96 to 706-102 PPC):

e) Capture of confidential words or private images

The capture of confidential words or private images is set out in articles 706-96 to 706-102 PPC.

Article 706-96

If the needs of an investigation into one of the penal infringements within the scope of articles 706-73 and 706-73-1 justify this, the liberty and custody judge may, upon request of the district prosecutor, authorise judicial police officer and agents to implement a technical device having the object, without the consent of the person concerned, caption, fixation, transmission and recording of words spoken privately or confidentially by one or several persons that are located in a private place.

In order to implement the technical device mentioned in the first paragraph of the current article, the liberty and custody judge may authorise the intrusion in a vehicle or a private place, including outside times mentioned in article 59, without the knowledge or without the consent of the owner or of the possessor of the vehicle or of the occupier or of any person having a right to this vehicle or place. These operations, which cannot pursue another aim than the one of implementing the technical device, are performed under his supervision. The current paragraph is also applicable to operations aiming to uninstall the implemented technical device.

The implementation of the technical device mentioned in the first paragraph cannot concern places mentioned in articles 56-1, 56-2, 56-3 and 56-5 and cannot take place in the vehicle, in the office or at the home of persons mentioned in article 100-7.

Article 706-96-1

If the needs of a judicial investigation into one of the penal infringements within the scope of articles 706-73 and 706-73-1 justify this, the investigating judge may, after having requested the opinion of the district prosecutor, authorise judicial police officer and agents to implement a technical device having the object, without the consent of the person concerned, caption, fixation, transmission and recording of words spoken privately or confidentially by one or several persons that are located in a private place.

In order to implement the technical device mentioned in the first paragraph of the current article, the investigating judge may authorise the intrusion in a vehicle or a private place, including outside times mentioned in article 59, without the knowledge or without the consent of the owner or of the possessor of the vehicle or of the occupier or of any person having a right to this vehicle or place. If a home is concerned and if the operation must take place outside times mentioned in article 59, this authorisation is delivered by the liberty and custody judge requested for this purpose by the investigating judge. These operations, which cannot pursue another aim than the one of implementing the technical device, are performed under the supervision of the investigating judge. The current paragraph is also applicable to operations aiming to uninstall the implemented technical device.

The implementation of the technical device mentioned in the first paragraph cannot concern places mentioned in articles 56-1, 56-2, 56-3 and 56-5 and cannot take place in the vehicle, in the office or at the home of persons mentioned in article 100-7.

Article 706-97

Authorisations mentioned in articles 706-96 and 706-96-1 are subject of a written and reasoned order which mentions all the details that enable to identify vehicles or private or public places concerned, the penal infringement that justifies the operation and the duration of operations. This order is not a jurisdictional decision and cannot be appealed.

Article 706-98

The authorisation decision taken pursuant to article 706-96 is delivered for a maximum duration of one month, renewable once under the same conditions.

The authorisation decision taken pursuant to article 706-96-1 is delivered for a maximum duration of two months, renewable under the same conditions, without the total period of operations being longer than two years.

Article 706-98-1

The operations provided for in articles 706-96 and 706-96-1 are carried out under the authority and the supervision of the magistrate who authorised them.

The fact that these operations reveal penal infringements other than those mentioned in these decisions is not a cause for nullity of incidental proceedings.

Article 706-99

The district prosecutor, the investigating judge or the judicial police officer appointed pursuant to articles 706-96 and 706-96-1 may require any qualified agent of a service or unit or body placed under the authority or supervision of the Ministry of the Interior or of the Ministry of Defence, a list of which is determined by means of a Decree, in order to install the technical devices mentioned in articles 706-96 and 706-96-1.

Article 706-100

The district prosecutor, the investigating judge or the judicial police officer appointed pursuant to articles 706-96 and 706-96-1 draws-up an official record of each of the operations of installation of the technical device and of the operations of capture, fixation, and sound or audio-visual recording. This official record mentions the date and times when the operation started and the date and time when the operation ended.

Recordings are placed under closed official seals.

Article 706-101

The district prosecutor, the investigating judge or the judicial police officer appointed pursuant to articles 706-96 and 706-96-1 describes or transcribes, in an official record attached to the case file, the recorded images and conversations that are useful to ascertain the truth. No sequence relating to private life but that has no relation with penal offences referred to in the decisions that authorise the measure can be kept in the case file.

Conversations in foreign language are transcribed into French with the assistance of an interpreter appointed for this purpose.

Article 706-101-1

The liberty and custody judge who authorised the operation mentioned in article 706-96 is informed without undue delay by the district prosecutor about acts that have been accomplished pursuant to this same article 706-96 and about official records that have been drawn-up pursuant to articles 706-100 and 706-101.

Article 706-102

The sound or audio-visual recordings are destroyed, at the initiative of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution. An official record is made of the destruction.

f) Interception of the content of the information accessed by users of electronic communications operators' services

The interception of the content of the information accessed by users of electronic communications operators' services is set out in articles 60-2 (flagrancy investigation), 77-1-2 (preliminary investigation), and 99-4 (judicial investigation, which means investigation procedure conducted by an investigating judge) PPC.

Article 60-2, §2 *et seq*.

A judicial police officer, acting upon orders of a district prosecutor authorised in advance by an order from the liberty and custody judge, may require telecommunications operators, particularly those mentioned in 1 of I of article 6 of Law no. 2004-575 of 21 June 2004 relating to confidence in the digital economy,[183] to take without delay all appropriate measures to ensure the preservation, for a period that may not exceed one year, of the content of the information accessed by persons using the services provided by the operators.

The organisations or persons to which this article applies must make the required information available as quickly as possible by means of telecommunication or computers.

Refusal to respond to such a request without a legitimate reason is punished by a fine of €3750.

[…]

Article 77-1-2, §2 *et seq*.

On the authorisation of the liberty and custody judge, seized to this end by the district prosecutor, a police officer may carry out the measures provided for in the second paragraph of article 60-2.

The organisations or persons concerned make the required information available as quickly as possible, by means of telecommunication or computers.

Refusal to respond to such a request without a legitimate reason is punished subject to the provisions of the fourth paragraph of article 60-2.

Article 99-4, §2 *et seq*.

With the express permission of the investigating judge, a judicial police officer may issue the demands provided for in the second paragraph of article 60-2.

The organisations or persons concerned must put the requisite information at their disposal by telecommunication or by use of computers as quickly as possible.

Refusal to respond to these demands without legitimate grounds is punished in accordance with the provisions of the fourth paragraph of article 60-2.

---

[183] These persons are Internet access service providers.

2. Scope of application

The object of interception and the temporal limits of electronic communications are subject to some matters of dispute.

a) Object of interception and temporal limits of electronic communication

The subject-matter of the interception and the temporal limits of the protection of electronic communications are different, depending on the procedure that is followed.

aa) Correspondence interception

In the above-mentioned provisions relating to correspondence interceptions, the legal subject-matter of the interception is correspondence transmitted by means of electronic communications. This statement implies to clarify below the notion of correspondence, the object of the legal protection, the temporal scope of this protection and the difference between legal regimes that enable correspondence interception.

(1) The notion of electronic correspondence

The notion of "electronic correspondence," as well as the notion of "correspondence" more widely do not have any comprehensive legal definition.[184] Correspondence has been defined by the legal literature as being "personal[185] and actual (present)[186] communications, which allow interactivity,[187] and which are addressed to determined and individualised persons."[188] These latter criteria of "determined and

---

[184] French law only evokes "private correspondence" in a negative way, within the provisions dedicated to public communications (art. 1, IV, subparas. 3 and 4 of Law n° 2004-575 of 21 June 2004 regarding confidence in the digital economy (called "LCEN"): "Public communication using electronic means shall mean any sign, signal, writing, image, sound or messages of all kinds, which are made available to the public by electronic means, and which have not the character of a private correspondence"; "Online public communication shall mean any transmission, on individual request, of digital data that have not the character of a private correspondence […]."

[185] A correspondence is "personal" where it is adapted to the recipient, in other words where it is "shaped according to" this "determined reader": Estelle De Marco*, L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT, n° 636, referring to Virginie Peltier, *Le secret des correspondances* (Correspondence secrecy), PU d'Aix-Marseille 1999, n°300.

[186] A correspondence is "actual" or "present" when it belongs to a determined period of time, where it has not lost its benefit due to the passage of time: Virginie Peltier, *Le secret des correspondances* (Correspondence secrecy), *op. cit.*, n° 300; Estelle De Marco*, L'anonymat sur Internet et le droit*, *op. cit.*, n° 636–637.

[187] Estelle De Marco*, op. cit.*, n° 631; Virginie Peltier, *op. cit.*, n° 222 and n° 15.

[188] Estelle De Marco*, op. cit.*, n° 632; Virginie Peltier, *op. cit.*, n° 15 p. 45.

individualised" persons were proposed in a ministerial circular of 17 February 1988,[189] and have been confirmed by the French data protection authority, together with the fact that correspondence of legal person is also protected.[190] As a result, this definition may be considered as applying to correspondence that is protected under the Penal and Penal Procedure Codes, as a minimum for what concerns the criteria of personal nature and temporality.

(2) Object of the protection

The protection granted to correspondence is supposed to benefit both the information medium and the information that is communicated, according to doctrine.[191]

Protected formats are supposed to be those mentioned in the definition of electronic communications, namely "signs, signals, writing, images or sounds."[192]

As regards technologies concerned by the powers granted to the judiciary in terms of correspondence interception, they are supposed to cover all technologies that enable the emission, transmission or reception of correspondence by electromagnetic means, according to the legal definition of electronic communication[193]. As a consequence, analogous communication (voice and data) may be intercepted via landlines and IP traffic of a person-to-person-communication, including through a mobile broadband modem.[194]

Finally, the components of correspondence that benefit from the protection of correspondence secrecy were clarified by the law of October 2016, according to which the protection covers "the content of the correspondence, the identity of correspondents and, where applicable, the title of the message and the documents enclosed to the correspondence."[195]

---

189 Circulaire du 17 février 1988 prise en application de l'article 43 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication (…), JORF of 9 March 1988, p. 3149.

190 The criteria of "determined and individualised persons," which might be legal persons, has been taken-up by the French Data Protection Authority in 2017 : CNIL, *Secret des correspondances : un consentement renforcé des utilisateurs de services de communication électronique* (Correspondence secrecy : a reinforced consent of users of electronic communication services), 31 March 2017, https://www.cnil.fr/en/node/23498

191 Estelle De Marco, *op. cit.*; Virginie Peltier, *op. cit*.

192 Art. L. 32-1 PECC, which defines "electronic communications" as "emissions, transmissions or reception of signs, signals, writings, images or sounds, by electro-magnetic means."

193 Art. L. 32-1 PECC, see preceeding footote.

194 Court of Cassation, crim. ch., 8 July 2015, n°14-88457, https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/3648_8_32306.html.

195 Art. L. 32-3, I PECC, added by Law n° 2016-1321 of 7 October 2016 entitled "Loi pour une République numérique," JORF n° 0235 of 8 October 2016, text n° 1, art. 68.

(3) Temporal scope of the protection

Correspondence benefits from the protection of the Penal Code and from the interception regime set out in the Penal Procedure Code during the time of its transmission only. This has been clarified by the doctrine[196] and confirmed by the French Court of Cassation, which considers that messages that have been received by their recipients may be intercepted by procedures other than the one dedicated to correspondence intercept, and particularly the search and seizure procedure.[197] Before and after transmission, correspondence still benefits from some protection, which is, however, lower.[198]

(4) Legal regimes enabling correspondence interception

Correspondence interception may be authorised under three different procedures, depending on the means used to implement it. Articles 100 to 100-8 and 706-95 PPC are the main provisions to be used to intercept correspondence, particularly on networks; articles 706-95-4 to 706-95-10 PPC enable the intercept of correspondence as it is sent or received by terminal equipment, and article 706-95-1 PPC enables the interception of correspondence stored in a mailbox by means of the use of an electronic identifier.

bb) Interception of private communications

Correspondence that has not yet been sent by its sender or that has been received by its recipient benefits from a lower protection than that afforded to correspondence in the course of its transmission. Its violation may be sentenced under civil law (article 9 CC) but is not made a specific penal offence. The interception of such correspondence is also less stringent, and may be implemented, depending on the interception means used, under the search and seizure procedure or under the procedure that enables the access of emails in a mailbox without the knowledge of its owner, by means of the use of an electronic identifier, under article 706-95-1 PPC.[199]

More globally, the search and seizure procedure enables the access of all types of stored public and private communications, as long as they are not considered being correspondence under transmission. Information accessed during internet surfing

---

196 Estelle De Marco, *op. cit.*, not. n° 641; Virginie Peltier, *op. cit*.

197 See, e.g., Court of Cassation, criminal chamber, 8 July 2015, n° 14-88457, bull., available at https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/3648_8_32306.html; Court of Cassation, criminal chamber, 9 March 2016, n°14-84566, bull., available at https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000032193829&fastReqId=1781896582&fastPos=1

198 See below, Section bb.

199 See below, Section b.aa.

may be intercepted using the procedure that allows the interception of the content of the information accessed by users of electronic communications operators' services, which follows the requisitions legal regime (articles 60-2, 77-1-2 and 99-4 PPC).[200]

cc) Remote data, words and image capture

All types of public and private electronic and audio-visual communications, including correspondence, may also be intercepted under the provisions that enable remote data capture, namely articles 706-102-1 to 706-102-9 PPC, since the subject-matter of the interception is any computer data exactly as it is displayed on the screen of the user of the computer system, or as it is typed by the user of the system, or as it is transmitted or received by audio-visual devices.

Confidential words and private images may in addition be intercepted under articles 706-96 to 706-102 PPC. As already discussed in this report,[201] this interception procedure is not strictly speaking an electronic communications interception, but it might lead in practice to the capture of the voice of one person speaking with another using electronic communication means, of meaningful images of this person in relation to the content of an ongoing call, or of the image and voice of a remote discussion partner, displayed through terminal equipment.

dd) IP traffic between a person and a computing system or between computer systems

Other types of private communications, such as IP traffic between a person and an automated information system,[202] IP-traffic between a person's computer and a data storage repository in a cloud or in another remote storage capability, and IP traffic between two independent computer systems (e.g., between an automated machine and its computer-based automated control centre), may also be intercepted through some procedures provided for in the Penal Procedure Code, such as the search and seizure procedure, the procedure enabling remote computer data capture (articles 706-102-1 to 706-102-9 PPC) and the special procedure that requires electronic communications operators to preserve the content of the information accessed by their users (articles 60-2, 77-1-2, and 99-4 PPC).

---

200 See below, Sections III.C. and D.

201 See above, Section II.A.1.d.

202 Such as communication with a webserver while uploading or downloading the content of a website.

b) Current matters of dispute

aa) The notion of "transmission" of correspondence

The notion of transmission determines the level of protection granted to correspondence. This implies the clear determination of the beginning and end of a transmission. This question is particularly pertinent to a mailbox, where emails may be found that have been written but not sent, emails received but not yet read by their recipient, and emails received and read by the latter. The related question in this case is whether correspondence stored by a hosting provider, in a traditional mail box or on a social network, should be intercepted using the correspondence interception procedure or if it may be accessed via a search and seizure procedure.

A legal analysis performed in accordance with the doctrinal definition of correspondence and the principles enshrined in the decisions of both the French Constitutional Council and the ECtHR leads to the conclusion that correspondence is protected as soon as the sender has initiated the sending of his or her correspondence, until this correspondence has been received by the addressee as a person. During this timeframe, no correspondence should be accessed outside the procedure set-up for correspondence interception, whatever its medium of transmission and its medium of storage.

Indeed, the initiation of the sending should be understood as a positive act of sending (such as an order to send made to a carrier), that the sender assumes to be effective.[203] As a result, any failure of transmission due to the carrier of the message should not prevent the correspondence from being protected. In particular, the protection should remain effective where a technical issue has temporarily prevented the actual sending and that the message stays in the outbox. Similarly, a message announcing the failure of the delivery enclosing the concerned message should be protected until the sender becomes aware of this failure and is granted with the power to delete the message or to send it again. Reception of the correspondence should be understood as a reception, by the addressee as a person, of "the last piece of information."[204] As a result, correspondence delivered in a medium of storage, whether the medium enables online visualisation or the storage of the message until the recipient downloads it, should not be considered being deliv-

---

[203] The secret of correspondence protects the freedom to correspond and the secrets a person is willing to share with another. These two actions suffer from the constraint to recourse to an intermediary to execute the conveyance of the message to be shared (see Virginie Peltier, *op. cit.*, n° 9 and 10). This should imply that correspondence is primarily protected during the time the message is under the control of this intermediary, which is the case at the very moment the sender entrusts it with his or her message, without regard to the moment the intermediary will effectively begin the sending technically speaking, or even without regard to the decision of this intermediary to postpone the sending due to an element of context that the sender – who dispossessed themselves of their message – does not know.

[204] Virginie Peltier, *op. cit.*, p. 471.

ered until this recipient has seen the correspondence and decided to delete it, to download it or to leave it stored on the server. In this regard, a message stored in a telephone messaging system has also been considered by the doctrine as correspondence.[205] This analysis, which seems to be clearly implied by the definition of correspondence, is also confirmed by article 226-15 PC, which states that correspondence is protected whether or not it has "arrived at their destination," the destination of correspondence being the recipient as a person, the mail box of the recipient being only a tool that enables correspondence reception but not a destination in itself. Such an analysis is also confirmed by recital n° 27 of Directive 2002/58/EC,[206] transposed under French law, according to which "the exact moment of the completion of the transmission of a communication […] may depend on the type of electronic communications service that is provided. […] For electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider."[207]

However, the Court of Cassation has stated in several decisions that the content of a mailbox may be subject to a search and seizure procedure. These decisions have mostly concerned seizures performed on the basis of article L. 450-4 of the Commerce Code, which provides for a specific search and seizure procedure that can be implemented by investigating services of the competition authority upon authorisation of the liberty and custody judge.[208] Within this framework, the Court of Cassation has also considered that the content of a mailbox is unbreakable,[209] that it may be globally seized as soon as it includes elements partly useful to prove alleged wrongdoing,[210] and that the irregular seizure of certain files or documents (such as correspondence exchanged between an advocate and their client) has no effect on the validity of the operations of search and of the seizure of other materials.[211]

---

[205] See Virginie Peltier, *op. cit.*, n° 14 p. 42.

[206] Directive 2002/58/EC of 12 July 2002, J.O.C.E. n° L. 201 of 31 July 2002, p. 37.

[207] On the discussion see Estelle De Marco, *L'anonymat sur Internet et le droit*, *op. cit.*, n°641.

[208] Court of Cassation, crim. ch., 9 March 2016, n°14-84566, bull., https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000032193829&fastReqId=1781896582&fastPos=1; Court of Cassation, crim. ch., 23 November 2016, n°15-81131, https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000033483607; Court of Cassation, crim. ch., 20 December 2017, n°16-83469, https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000036343934; Court of Cassation, crim. ch., 4 May 2017, n°16-81062, https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000034653409&fastReqId=1731033929&fastPos=3

[209] Court of Cassation, crim. ch., 20 December 2017, *op. cit*.

[210] Court of Cassation, crim. ch., 23 November 2016, *op. cit*.

[211] Court of Cassation, crim. ch., 4 May 2017, *op. cit.*; Court of Cassation, 20 December 2017, *op. cit.*

In a decision of 8 July 2015[212] related to judicial investigations, the Court of Cassation made a clear distinction between emails received from the date of a written decision of correspondence interception taken by an investigating judge, which are subject to this very procedure, and emails "sent or received" before the date of this interception decision, which "collection, registration and transcription […] must be performed in compliance with provisions regulating seizure,"[213] in particular where this correspondence has been "stored before the date" of this written decision.[214]

No one of the above-mentioned decisions made a distinction between emails actually received by the recipient (and therefore opened by the recipient), emails technically received by the hosting provider but not opened by the recipient, and emails written by the owner of the mailbox but standing in an outbox or returned due to a delivery failure not yet known about by the mailbox owner.

This position of the Court of Cassation is questionable, since the search and seizure procedure does not provide for sufficient guarantees in relation to correspondence protection. As a result correspondence stored in a mailbox should not be intercepted using means other than the correspondence interception procedure or another procedure offering similar guarantees, if not higher. This principle should at least concern correspondence that is being sent and correspondence that has not been opened by the recipient person, and should by extension concern the entire contents of a mailbox, where there is no practical possibility to access voluntarily stored correspondence without having knowledge of correspondence that is still under transmission.

The sole advantage of the search and seizure procedure, compared to the interception procedure, is that it is in principle performed in the presence of the owner of the mailbox, whereas the interception procedure is secret.[215] However, this benefit remains theoretical since secret access to the content of emails may be admitted

---

[212] Court of Cassation, criminal chamber, 8 July 2015, n° 14-88457, bull., available at https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/3648_8_32306.html. Previously, the Court of Cassation considered that the content of mailboxes could be seized: see, e.g., Cour de cassation, ch. crim., 6 November 2013, n° 12-87130 (arrêt n° 5362), https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/5362_6_27718.html

[213] Translated from French: "l'appréhension, l'enregistrement et la transcription de correspondances émises ou reçues par la voie des télécommunications antérieurement à la date de la décision écrite d'interception prise par le juge d'instruction […] doivent être réalisés conformément aux dispositions légales relatives aux perquisitions."

[214] Translated from French: "y compris celles stockées antérieurement à l'autorisation d'interception."

[215] See, e.g., on this issue J.P. Karsenty & associés, *Recueillement de données électroniques : interception de correspondances ou perquisition* ? [Gathering of electronic data; correspondence interception or judicial search?], 2015, https://www.jpkarsenty.com/Recueillement-de-donnees.html

as an investigating act,[216] and since French law has, since June 2016, authorised the secret seizure of the content of email boxes using a password.

bb) Direct access to mailboxes using their password

As we will analyse later, the law concerning the retention of connection data (see III.C. below) has since 2011 imposed the retention of certain information provided at the time of the contract subscription or of the creation of the users' account, including – only where the provider usually collects such information – the password and the data that enables the modification or verification of this password, in its latest and updated form.

The use of these passwords, which in practice enables the judiciary to gain access to email boxes and therefore to protected correspondence within the framework of investigations and search and seizure procedures, was not specifically regulated until Law n°2016-731 of 3 June 2016 which created article 706-95-1 PPC. This provision provides the liberty and custody judge and the investigating judge with the power, within the framework of a restrictive list of infringements qualified as organised crime and delinquency,[217] to authorise remote access to correspondence stored through electronic communication means, using an electronic identifier, without the owner of the mailbox being aware.

Among the difficulties posed by this provision lies the fact that the procedure to be followed for correspondence interception (described in articles 100 to 100-6) is not applicable, including the protection offered to journalists' sources provided in article 100-5, whereas at the very moment investigators gain access to the concerned mailbox there is a very high probability that correspondence under transmission will be included in it. In addition, safeguards surrounding the procedure appear to be lower than the safeguards that surround the search and seizure procedure, even though it is placed under the supervision of a judge. In particular, correspondence

---

[216] See, e.g., a decision of the Court of Cassation which validates the use of a password in order for investigators to access a private electronic space within the framework of an investigation, such action not requiring a specific authorisation from the judge who ordered the search and seizure procedure that enabled the discovery of the password (this decision could be extended to mailboxes): Court of Cassation, ch. crim., 6 November 2013, n° 12-87130, 6° moyen [ground of appeal], https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/5362_6_27718.html; in addition, the Court of Cassation has validated the possibility for investigators to obtain copies of emails from Google located in USA on the basis of a non-binding requisition: Court of Cassation, same decision, 2° and 3° moyens [grounds of appeal], comment available at https://www.legalis.net/actualite/enquete-preliminaire-validation-de-requisitions-directes-de-donnees-aupres-de-google-inc/. Previously, the Court of Cassation considered that a request for the content of emails addressed to operators located in France was irregular, but was not a cause for nullity since no email had been transcripted (which is contestable since secrecy of correspondence may have been violated): Cour de cassation, crim. ch., 22 October 2013, https://www.legalis.net/jurisprudences/cour-de-cassation-chambre-criminelle-arret-du-22-octobre-2013/

[217] Listed in arts. 706-73, 706-73-1 and 706-72 PPC, see above, Section III.B.7.b.

that is accessed can be "seized and registered or stored on any support," according to article 706-95-1, which offers a significantly lower level of protection than closed seals.[218] More importantly, the owner of the mailbox does not participate in the seizure and in the closing of seals.

Furthermore, a difference of protection can be noted between stored correspondence that is accessed through the use of an electronic identifier and stored correspondence that is seized during a traditional search and seizure procedure, whereas in both cases the nature as correspondence or as correspondence under transmission is the same.[219]

3. Special protection of confidential communication content

Correspondence can only be intercepted under particular conditions when its sender or recipient practices certain occupations. Similarly, certain places such as the home, the business premises, and sometimes the vehicle of certain persons, due to their functions, are protected from the implementation of technical devices that enable certain kinds of interceptions. In addition, some types of correspondence are protected against transcription.

a) Privileged correspondence

Article 100-7 PPC provides special protection for Members of Parliament, advocates, judges, and prosecutors. This article states that, under penalty of nullity,

– no interception may be made on the telephone line of a Member of Parliament or senator unless the president of the assembly he belongs to is informed of the interception by the investigating judge;
– no interception may be made on a telephone line connecting the chambers or domicile of an advocate unless the president of the bar association is informed of this by the investigating judge; and
– no interception may be made on a telephone line connecting the chambers or domicile of a judge or prosecutor unless the president or the prosecutor general of the court with jurisdiction over the area in question is informed of this by the investigating judge.

This provision is applicable within the framework of all interception procedures[220] with the exception of the procedure that enables the interception of the

---

[218] Required in art. 56 PPC in relation to search and seizure.

[219] In relation to the distinction between correspondence and correspondence under transmission, see above, Sections 2.a.aa. and bb. and 2.b.aa.

[220] See art. 706-95-3 PPC in relation to the access to mailboxes using an electronic identifier, arts. 706-95-4 and 706-95-5 PPC in relation to interception of correspondence sent or received by terminal equipment, art. 706-96 PPC in relation to remote capture of confi-

information accessed online (which may concern any person).[221] It also protects the vehicle, home and business premises of persons mentioned in article 100-7 against the implementation of an intrusion device enabling remote capture of data, confidential words or private images.[222] Home and business premises (with the exclusion of the vehicle) of the same persons are also protected from the implementation of a geolocation device,[223] but not from the implementation of a technical device that enables the collection of technical connection data including geolocation of terminal equipment.[224]

In addition, articles 56-1 to 56-3 and article 56-5 PPC protect particularly, within the framework of judicial search and seizures, certain other places which are also protected from geolocation, remote data capture, and remote capture of private images and confidential words.[225] These places are the following (and can only be the subject of a search and seizure procedure under strict conditions):

– the business premises and the home of an advocate;
– the business premises and professional vehicles of media companies, audiovisual communication companies, online public communication companies and press agencies;
– the home of a journalist;
– the professional premises of medical doctors, notaries, or bailiffs;
– court premises and the home of persons exercising judicial functions.

Furthermore, where a requisition of electronic documents or information concerns the persons mentioned in these articles 56-1 to 56-5,[226] the delivery of required documents and information can only take place with their agreement.[227]

---

dential words or private images, art. 706-102-5 in relation to remote data capture of information as it is stored or displayed on a computer or sent or received by this computer.

221 Arts. 60-2, 77-1-2, and 99-4 PPC.

222 Art. 706-96 PPC related to remote capture of confidential words or private images and art. 706-102-5 related to remote data capture of information as it is stored or displayed on a computer or sent or received by this computer. Both provisions clarify that the implementation of the technical device that enables such operations cannot be done in the vehicle, home or business premises of persons mentioned in art. 100-7.

223 Art. 230-34 PPC.

224 Arts. 706-95-4 and 706-95-5 PPC. See below, Section III.C.1.

225 Arts. 230-34 (geolocation), 706-102-5 (remote data capture) and 706-96 (remote capture of private images and confidential words), by reference to the places mentioned in arts. 56-1 to 56-3 and 56-5 PPC.

226 Art. 56-4 PPC protects in addition, in this particular situation, places where information relating to national defence is stored.

227 Arts. 60-1, 77-1-1, and 99-3 PPC

b) Prohibition of transcription of certain types of correspondence

In addition to the rules described above, article 100-5 PPC states that, on penalty of nullity:

– no transcription may be made of any correspondence with an advocate relating to the exercise of the defendant's rights, and
– no transcription may be made of any correspondence with a journalist allowing identifying a source in breach of article 2 of the Law of 29 July 1881 on freedom of the press.

This provision is applicable within the framework of remote correspondence intercept on networks[228] and on the computer used to send or receive the correspondence.[229]

However, this provision does not prevent the judicial police officer in charge of the implementation of the measure to hear or read conversations, which renders the protection somewhat inexistent, in practice, in the absence of stronger guarantees surrounding operations where secrets are exchanged.

In addition this provision is not applicable within the framework of the procedure that enables the interception of information accessed online,[230] whether accessing a mailbox using a password,[231] using remote data capture[232] or remote capture of confidential words or images.[233]

- Regarding the interception of the information accessed online, provisions only stipulate that a protocol between the relevant ministry and the persons in charge to implement the interception must clarify, *inter alia*, the "guarantees that enable to limit the access to the sole requested information and to prevent any access to information protected by a secrecy provided for by law, especially by medical secrecy, outside the cases where this secret cannot be opposed to the judicial authority."[234]
- Regarding access to a mail box using a password, provisions are silent in relation to protected correspondence and state only that accessed data is "seized and registered or copied on any support," [235] and that these operations cannot "have

---

228 Arts. 100 to 100-8 and 706-95 PPC.
229 Arts. 706-95-4 and 706-95-5 PPC.
230 Arts. 60-2, 77-1-2, and 99-4 PPC.
231 Arts. 706-95-1 to 706-95-3 PPC.
232 Arts. 706-102-1 to 706-102-9 PPC.
233 Arts. 706-96 to 706-102 PPC.
234 Art. R. 15-33-72, 6°, adopted pursuant to arts. 60-2, 77-1-2, and 99-4 PPC.
235 Arts. 706-95-1 and 706-95-2 PPC.

another object than search and ascertainment of the infringements referred to in the decision"[236] authorising the measure.

- Regarding the two other procedures, provisions only state that "no sequence relating to private life alien to the infringements referred to in the decision authorising the measure can be kept in the case file."[237]

In this context, judges might at least partly[238] follow the Court of Cassation's jurisprudence relating to seized elements of a mailbox that have no links with the object of the decision the search was based upon. In such a situation, the Court of Cassation considers a mailbox an unbreakable file, as previously analysed in this report.[239] As a result this Court has ruled, in relation to search and seizure procedures implemented by investigating services of the competition authority upon authorisation of the liberty and custody judge, that the fact that a mailbox contains some elements that are covered by the decision authorising search and seizure is sufficient to make the global seizure valid.[240] However, the presence of protected information[241] or of information that has no link with the object of the authorisation,[242] even though it does not invalidate the seizure, must lead the judge to quash the seizure in relation to this protected information only[243] and must lead the ad-

---

236 Art. 706-95-3 PPC.

237 Arts. 706-101 and 706-102-8 PPC.

238 It might at least concern information collected during remote capture of computer data or of confidential words or private images, since the device that enables such collection cannot be implemented in places mentioned in articles 56-1 to 56-3 and 56-5 PPC (see a. above), the respect of these same articles being required within the framework of the search and seizure procedure. Mention of these articles does not appear in the provisions that enable the interception of the information consulted online and that enable the use of a password for accessing a mailbox (in this latter case, only advocates, magistrates and Parliament members benefit from a protection through the application of the provisions of article 100-7: see above, Section a. and below, Appendix.

239 See above, Section III.B.2.b.aa.

240 Court of Cassation, crim. ch., 4 May 2017, n° 16-81062, available at https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT00003465 3409&fastReqId=1731033929&fastPos=3; Court of Cassation, crim. ch., 20 December 2017, n° 16-83469, available at https://www.legifrance.gouv.fr/affichJuriJudi.do? old Action=rechJuriJudi&idTexte=JURITEXT000036343934; Court of Cassation, crim. ch., 23 November 2016, n° 15-81131, available at https://www.legifrance.gouv.fr/affich JuriJudi.do?idTexte=JURITEXT000033483607. See also CA [Court of appeal] Versailles, 19 February 2010, *Janssen-Cilag v. Autorité de la concurrence et autres*, available at https://www.legalis.net/jurisprudences/cour-dappel-de-versailles-ordonnance-du-19-fevrier-2010/

241 Court of Cassation, crim. ch., 4 May 2017, *op. cit.*; see also CA Versailles, 19 February 2010, *op. cit.*

242 Court of Cassation, crim. ch., 23 November 2016, *op. cit.*; see also CA Versailles, 19 February 2010, *op. cit.*

243 Court of Cassation, crim. ch., 4 May 2017, *op. cit.*; Court of Cassation, 20 December 2017, *op. cit.*

ministration to return this very information to the people seized,[244] or, where this return is impossible, to not report this information.[245]

One issue is, however, that, in order to enable the above-mentioned seizure annulment and information return, the person whose information has been seized receives a copy of the seized information,[246] and it is their responsibility to identify precisely the information that is protected by a particular secret or that has no link with the object of the seizure, if this is not obvious,[247] and to request the return of this information from the administration.[248] Such identification and request for annulment and return are not possible within the framework of interception of information consulted, of access to a mailbox using a password and of remote capture of data or of words and images, since these procedures are implemented without the concerned person being aware of it.

In conclusion, the protection of certain persons due to their functions, particularly advocates and journalists, seems rather low, which is a particularly concerning issue given the crucial roles of these functions in a State governed by the rule of law, within the context of the existence of article 40 PPC, which imposes on any public agent the duty to report to the district prosecutor any crime or misdemeanour discovered upon exercising his or her powers, along with related information.[249]

4. Execution of electronic communications interception

The execution of electronic communications interception may be performed by qualified persons under the judge's supervision, by means of several techniques.

a) Execution by the authorities with or without the help of third parties and accompanying powers

As explained previously, provisions that regulate correspondence interception and data capture provide for a mode of execution that is superseded by the use of the national platform for judicial interceptions where technology allows it.

---

244 CA Versailles, 19 February 2010, *op. cit.*

245 Court of Cassation, crim. ch., 20 December 2017, *op. cit*.

246 Court of Cassation, crim. ch., 4 May 2017, *op. cit.*; see also CA Versailles, 19 February 2010, *op. cit.*

247 Court of Cassation, crim. ch., 23 November 2016, *op. cit.*; see also Court of Cassation, crim. ch., 4 May 2017, *op. cit.*, and CA Versailles, 19 February 2010, *op. cit.*

248 CA Versailles, 19 February 2010, *op. cit.*

249 See above, Section II.A.3.

aa) Execution of data interceptions according to statutory provisions

Provisions that regulate correspondence interception and access to stored correspondence by the means of the use of a password are performed by the judge or by the judicial police officer appointed by him, but the latter may request the assistance of any qualified agent belonging to a service or body placed under the authority of the ministry in charge of electronic communications, or any qualified agent belonging to an authorised electronic communications service.[250] The execution mode is thus determined by the judge who authorised and supervises operations.

Regarding remote connection data capture including correspondence interception at the level of terminal equipment,[251] the "apparatus or technical device" that enables the interception of communications is in principle operated by a judicial police officer but the latter, as well as the judge and the district prosecutor may request the assistance of any qualified agent belonging to a service or unit or body placed under the authority or supervision of the Ministry of the Interior and of which a list is determined by means of a decree.[252] The notion of "technical device" must be understood, within the framework of this procedure, as any "hardware or software,"[253] but it mainly referred, in the legislator's intent, to "proximity technical device" (also called an IMSI catcher),[254] which explains that the provisions surrounding the exercise of this power do not provide for the possibility for the judge to authorise an intrusion into private or professional places where data must be captured.

Similar rules govern confidential words and private image capture[255] in relation to the persons authorised by law to implement the technical device that will enable

---

250 Arts. 100-3 and 706-95-3 PPC.

251 Arts. 706-95-4 and 706-95-5 PPC.

252 Art. 706-95-8 PPC. The list of competent services is available in art. D15-1-5-1 PPC.

253 Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal [Administrative decision determining the list of apparatuses and technical devices, provided for in article 226-3 PC], Annex 1, modified, available at https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=6BB0AE272 provisions that regulate correspondence interception B2AC4D0F771ED8BAE7E76E9. provisions that regulate correspondence interception tplgfr38s_1?idArticle=LEGIARTI provisions that regulate correspondence interception 000033064127&cidTexte= provisions that regulate correspondence interception JORFTEXT000026241910&categorieLien=id&date Texte=20160930. Indeed, arts. 706-95-4 and 706-95-5 provide for the use of apparatuses or devices described in art. 226-3 PC in order to intercept communications, the use of these apparatuses and devices being prohibited outside the framework of authorised judicial or administrative interceptions.

254 See Décret n° 2016-1159 du 26 août 2016 pris pour l'application de l'article 706-95-8 du code de procédure pénale [Decree n° 2016-1159 of 26 August 2016 issued for the purpose of the application of article 706-95-8 PPC], foreword, JORF n° 0199 of 27 August 2016, text n° 20, available at https://www.legifrance.gouv.fr/eli/decret/2016/8/26/INTD 1623640D/provisions that regulate correspondence interception jo/texte

255 Arts. 706-96 to 706-102 PPC.

the interception.[256] Since the wording of "technical device" is the same as in the provisions regulating the other powers, it is supposed to refer to hardware and software mechanisms as well. Provisions related to this procedure enable the judge to authorise an intrusion into private places where voice and images must be captured, being silent in relation to other possible means of implementation. Regarding remote data capture,[257] the installation of the technical device that is necessary to perform operations is in principle performed by the judge, the district prosecutor or a judicial police officer appointed for this purpose, but any of these persons may request the assistance of a qualified agent belonging to a service or unit or body placed under the authority or supervision of the Ministry of the Interior or of the Ministry of Defence, a list of which is determined by means of a decree.[258] In addition, the district prosecutor or the investigating judge may require any natural or legal person who is authorised and mentioned in one of the lists mentioned in article 157 PPC[259] order to execute the technical operations that are necessary to implement the technical device.[260] The notion of "technical device" is not defined in relation to this procedure, but articles 706-102-4 and 706-102-5 PPC clarify that the judge may authorise the transmission of the device by the means of an electronic communication network, in addition to their power to authorise an intrusion into private places where data must be captured, which implies that the notion both refers to hardware and software materials, and that the device may be installed physically in the concerned private place or transmitted electronically.

Finally, a request addressed to electronic communication operators to ensure the preservation of information consulted by their users without delay can be issued by the district prosecutor, a judicial police officer (upon authorisation of the district prosecutor in case of preliminary investigation) or the investigating judge. The provision of the information must take place without undue delay by telematic or computing means.[261]

---

256 Art. 706-99 PPC.

257 Arts. 706-102-1 to 706-102-9 PPC

258 Art. 706-102-6 PPC. The list of competent services is available in art. D15-1-6 PPC.

259 Art. 157 PPC refers to experts mentioned in the national list established by the Court of Cassation or in one of the lists established by the courts of appeal, in compliance with conditions surrounding the designation of judicial experts.

260 Arts. 706-102-1, §2 and 706-102-2, §2 PPC

261 Arts. 60-2, §2, 77-1-2, §2 and 99-4, §2 PPC. See above, Section III.B.1.f.

bb) Execution of data interceptions through the national platform for judicial interceptions

Since 2016, article 230-45 PPC[262] has stated that unless technically impossible, a certain number of interception measures must be transmitted through a national platform for judicial interceptions,[263] which organises the centralisation of their execution. This platform is placed under the authority of the Ministry of Justice[264] and has been progressively established since 2014.

In relation to the interception of the content of communications during their transmission outside traffic and location data, the concerned communications interceptions are correspondence interception[265] and requests for preservation of and access to the content of the information accessed by users of electronic communication services.

In addition, correspondence interception at the level of the terminal equipment[266] will also have to be centralised and stored in this national platform for judicial interceptions, unless technically impossible, under the modalities determined by a decree adopted in the Council of State.[267]

Functioning modalities of the platform are described in articles R. 40-42 to R. 40-56 PPC. Requisitions from judges and judicial police officers are transmitted to requisitioned stakeholders by the platform following a protocol described in article R. 15-33-72 PPC. The platform receives answers and makes them available to the judge or judicial police officer who made the request.[268] Information that can be registered is listed in article R. 40-46. Any operation relating to the processing is registered, along with the identification of the user, the date, the time, and the nature of the operation, for a five-year period.[269]

---

[262] Created by Law n°2016-731 of 3 June 2016, Art. 88, JORF n°0129 of 4 June 2016. Art. 230-45 has been later modified by Law n°2017-258 of 28 February 2017 (art. 35) and Law n° 2018-699 of 3 August 2018 (art. 16).

[263] Regulated, according to art. 230-45 PPC, by decree, which has been codified in arts. R. 40-42 to R. 40-56 PPC.

[264] Art. R. 40-42 PPC (Decree n°2014-1162 of 9 October 2014).

[265] Arts. 100 to 100-7, art. 706-95, art. 74-2, art. 80-4, and art. 709-1-3 PPC.

[266] Arts. 706-95-4 and 706-95-5 PPC.

[267] Arts. R. 40-42 to R. 40-56 PPC, which regulate the modalities of the recourse to the national platform for judicial interceptions, did not provide for their application to the measure regulated in arts. 706-95-4 and 706-95-5 PPC, at the time the current report was prepared.

[268] Art. R. 40-45 PPC.

[269] Art. R. 40-50 PPC.

b) Cross-border interception

Where an interception of correspondence transmitted by means of electronic communication, performed under articles 100 to 100-7 PPC, targets a communication address which is used in the territory of a Member State of the European Union, but does not take place within the framework of a European Investigation Order, the investigating judge or the judicial police officer appointed by him must notify[270] this interception to the competent authority of the State where the person concerned is located. Where such interception could not be authorised, within the framework of a similar national proceeding, under the law of that State, the interception cannot be carried out or it must be interrupted, or intercepted data while the person was in its territory cannot be used and must be removed from the record of the proceedings or can only be used under the conditions specified by this authority and for the reasons it specifies.[271]

Where a Member State of the European Union notifies the French State that it is performing or would like to perform an interception on a communication address used in the French territory and relating to a person that is physically in the French territory, the notification is addressed to the Director of criminal affairs and pardons of the Ministry of Justice. Where such interception could not be authorised, within the framework of a similar national proceeding, under the provisions of the French PPC, the Director of criminal affairs and pardons may, within 96 hours of receipt of the notification, request that the interception is not carried out or is interrupted, or that data intercepted while the person was in the French territory are not used or are used only under the conditions they specify and for the reasons they specify.[272]

Within the framework of the other procedures, provisions regulating each specific power do not provide for rules to be followed if the device to be intercepted is located in another country or is not geolocated with certainty. As a result the rules to be applied are those which regulate judicial assistance more generally.[273]

5. Duties of electronic communication service providers to cooperate

French law includes some general provisions that recall the duty of electronic communications service providers[274] – and more widely the duty of any citizen[275] –

---

[270] This notification is made by using the form that lies in Annex C of Directive 2014/41EU of 3 April 2014 regarding the European Investigation Order in criminal matters: art. D32-2 PPC, modified by Decree n°2017-511 of 7 April 2017.

[271] For further details, see Appendix, Section A., art. 100-8 PPC.

[272] Art. D32-2-1 PPC, created by Decree n°2017-511 of 7 April 2017.

[273] Arts. 694-14 *et seq*. PPC. See below, Section V.

[274] Art. L. 33-1, I, §§ 5 and 10 PECC that "the setting up and the exploitation of electronic communications networks are subject to the respect for rules relating to […]" public order, national defence and public security requirements, including rules that are necessary to the setting up of communications intercepts required for public security purposes.

to provide support to justice for the manifestation of the truth. More particularly, electronic communications operators[276] and Internet access providers[277] must take without delay all appropriate measures to ensure the preservation of the text of the information consulted by persons using the services they provide, when they are required to do so according to article 60-2 PPC. Refusal to respond to such a request without a legitimate reason is punishable by a fine of €3750.

Electronic communications operators have a general obligation, sometimes recalled by additional specific provisions relating to specific questions, to respect the rules relating to the protection of personal data,[278] the secrecy of correspondence,[279] and the confidentiality and neutrality of content transmitted using their networks.[280] These stakeholders are also obliged to ensure the integrity and the security of their networks.[281]

In addition, electronic communication operators must answer the requests made through the national platform for judicial interceptions[282] the purpose of which is to receive and store:

Art. L. 33-1, V states that electronic communication operators must enable judicial authorities, police and Gendarmerie services, file and rescue services and emergency medical aid services, executing their mission, to access their lists of subscribers and users, unredacted and up-to-date. Art. L. 32-1, II, § 7° also considers as a general objective (to be enforced by the Ministry for Electronic Communications and the regulatory authority) the respect by operators of the public order and of obligations of defence and public security.

275 Art. 10 CC states: "Everyone is required to lend his aid to the court so that the truth may be revealed. He who, without legitimate reason, evades that obligation when it is legally required of him, may be compelled to comply with it, if need be on pain of a periodic penalty payment or of a civil fine, without prejudice to the right to recover damages." See the English translation of the Civil Code on Legifrance (the French public service for the dissemination of law) at https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721&dateTexte=20160929

276 Electronic communications operators are defined in art. L. 32, § 15°PECC as "natural or legal persons who exploit an electronic communications network opened to the public or who provide the public with an electronic communications service" (the notion of "provision" being understood here as the transmission of electronic communications on a network).

277 Internet access providers are defined in art. 6, I, § 1 of Law 2004-575 of 21 June 2004 as "persons whose activity is to provide an access to online public communication services."

278 General rules are included in art. L. 32-1, II, § 6°PECC and in Law n°78-17 of 6 January 1978 modified. Specific obligations are, e.g., included in provisions relating to the retention of traffic data.

279 The general rule is included in art. L. 32-1, II, § 6° PECC and in art. 226-15 PC. Specific obligations are, e.g., included in art. L. 32-3 PECC, in addition to art. 432-9 PC which specifically sanctions correspondence violation where committed by electronic communications operators.

280 General rules are included in art. L. 32-1, II, §6° and L. 33-1, b) PECC. Specific obligations are, e.g., included in art. L. 32-3-3 of the same Code.

281 See, e.g., art. L. 33-1, a) PECC.

282 See above, Section III.B.4.a.bb.

– the content of electronic communications intercepted on the basis of articles 74-2, 80-4, 100 to 100-7, and 706-95 PPC;
– data and information communicated by service providers within the framework of three procedures: the procedure for the interception of the content of the information accessed by users of electronic communications operators' services (arts. 60-2 §2 *et seq*.; 77-1-2 §2 *et seq*., and 99-4 §2 *et seq*. PPC), the procedure for requesting traffic and connection data (arts. 60-1; 77-1-1, and 99-3 PPC), and the procedure for accessing, including remotely, information stored in computer and data processing systems (arts. 60-2, §1 and 5; 77-1-2 §1, and 99-4 §1 PPC).

6. Formal prerequisites of interception orders

As can be noted by reading statutory provisions relating to correspondence interceptions, remote data capture and interception of the content of the information accessed by the users of electronic communications networks, each of these procedures is governed by different rules.

a) Competent authorities

aa) Correspondence interception

(1) Correspondence interception under articles 100 *et seq*. PPC

In principle, based on articles 100 to 100-7 PPC, correspondence interception may be ordered by the investigating judge only, where the requirements of the investigation call for it, for the investigation of felonies and misdemeanours where the penalty incurred is equal to or in excess of two years imprisonment[283] or for searching for causes of death of disappearance.[284] The interception is made under the authority and supervision of this magistrate. Moreover, the judge responsible for enforcing sentences can order such correspondence interception, where one or several reasonable grounds enable the belief that a person, having served his sentence (applied for the same kinds of felonies and misdemeanours indicated above), does not respect the prohibition written in the initial sentence, of contacting certain persons visiting certain areas.[285] The judge responsible for enforcing sentences issues the order on his own initiative or, in some specific situations described by the Penal Code, on the request of the district prosecutor.

Additionally, the liberty and custody judge of the district Court may, where the requirements of the investigation call for it, on the request of the district prosecutor, order a correspondence intercept in the search for an escaping person. Correspond-

---

283 Art. 100 PPC.
284 Art. 80-4 PPC.
285 Art. 709-1-3 PPC.

ence interceptions are performed under the authority and supervision of this liberty and custody judge.[286] Finally, for the purpose of organised crime repression, in relation to a quite important list of felonies and misdemeanours,[287] the liberty and custody judge of the district Court may also order a correspondence interception, on the request of the district prosecutor, where the requirements of a flagrancy or preliminary investigation call for it.[288] In this latter situation, the applicable procedure (at the exclusion of conditions relating to the length of the measure[289]) is the one that governs correspondence interception under articles 100 to 100-7 PPC and the powers conferred to the investigating judge or to the judicial police officer appointed by him are exercised by the district prosecutor or to the judicial police officer appointed by this magistrate.

(2) Other types of correspondence interception

The other types of correspondence interception may only take place, in principle, in relation to organised crime and delinquency as defined in the Penal Procedure Code.[290]

Within this context, both the investigating judge (in the case of judicial information) and the liberty and custody judge of the district Court, upon request from the district prosecutor (in the case of a preliminary or a flagrancy investigation) are entitled to authorise the access to a mailbox using an electronic identifier[291] and[292] the use of a technical device (intended to be an IMSI catcher[293]) in order to intercept connection data and if necessary correspondence as it is received or sent by a terminal equipment. All these operations are performed under the authority and supervision of the judge who ordered them, and, if correspondence is intercepted, the formal prerequisite and execution conditions of articles 100-4 to 100-7 PPC [294] are applicable (and, where the measure is authorised by the liberty and custody judge, the powers conferred to the investigating judge or to the judicial police

---

286 Art. 74-2 PPC.

287 Listed in arts. 706-73 and 706-73-1 PPC. Additional provisions may also provide for the application of interception powers in relation to other infringements see below, Section III.B.7.b.

288 Art. 706-95 PPC.

289 Art. 100-2 PPC.

290 The misdemeanour or the crime must be one of those listed in arts. 706-73 and 706-73-1 PPC. As mentioned in a preceeding footnote, it might additionally happen that other provisions provide for the application of interception powers in relation to other infringements see below, Section III.B.7.b.

291 Arts. 706-95-1 to 706-95-3 PPC.

292 In this case the investigating judge must obtain the opinion of the district prosecutor (art. 706-95-5 PPC).

293 See above, Section III.B.4.a.

294 See above, Section III.B.6.a.aa.(1).

officer appointed by him are exercised by the district prosecutor or to the judicial police officer appointed by this magistrate).

In case of emergency resulting from an imminent risk of evidence being damaged or an imminent risk of serious harm to persons or goods, the decision to use a technical device in order to intercept connection data and if necessary correspondence as it is received or sent by terminal equipment may also be issued by the district prosecutor. In this case, the decision must be confirmed by the liberty and custody judge within 24 hours. Failing that, the operation is brought to an end, collected data or correspondence is placed under closed official seals and cannot be exploited or used in the proceedings.

bb) Remote data, voice and image capture

Computer data capture,[295] as well as capture of confidential words and images,[296] may only take place within the framework of the prevention of organised crime and delinquency as defined in the Penal Procedure Code.[297] These measures must be authorised by the investigating judge (after obtaining the opinion of the district prosecutor) or the liberty and custody judge of the district Court (at the request of the district prosecutor) and are implemented and performed under the authority and supervision of the judge who ordered them.

Where the measure can only take place by the means of an intrusion into a home outside the times prescribed in article 59 in relation to searches and house visits,[298] a specific authorisation to perform this intrusion must be delivered by the custody judge, seized to this end by the investigation judge where the latter is the one who authorised the data, image or voice capture,[299] or, within the framework of data capture, seized to this end by the district prosecutor.[300]

cc) Interception by service providers of the content of the information accessed by their users

The preservation of and access to the content of the information accessed by users of electronic communication services may be requested by a judicial police of-

---

295 Arts. 706-102-1 and 706-102-2 PPC.

296 Arts. 706-96 to 706-102 PPC.

297 The misdemeanour or the crime must be one of those listed in arts. 706-73 and 706-73-1 PPC. As mentioned in a preceeding footnote, it might additionally be the case that other provisions provide for the application of interception powers in relation to other infringements. See above, Section III.B.6.a.aa. and below, Section III.B.7.b.

298 Art. 59 states that, except where they are requested from within a building or in the exceptional cases provided for by law, searches and house visits may not be undertaken before 6 am or after 9 pm.

299 Art. 706-102-5 PPC.

300 Art. 706-96-1 PPC.

ficer acting upon authorisation of the liberty and custody judge (seized to this end by the district prosecutor) in a preliminary investigation situation,[301] by a judicial police officer acting upon orders of a district prosecutor (authorised in advance by a decision from the liberty and custody judge) in a flagrancy investigation situation,[302] and by a judicial police officer acting upon express authorisation of the investigating judge in situations of judicial information.[303]

b) Formal requirements for applications and orders

Requirements for applications and orders differ depending on the procedure that is followed.

aa) Correspondence interceptions

Provisions that are specific to correspondence interceptions do not particularly regulate the form of the requests made by the district prosecutor to the liberty and custody judge.

Correspondence interception orders from the liberty and custody judge or the investigating judge must be made in writing, must specify all the details identifying the link to be intercepted, the offence which justifies resorting to an interception and the duration of this interception.[304] These orders must moreover be issued within the strict framework described in the provision that enables each specific measure (it must, e.g., be required by the needs of the judicial information or investigation under article 100 PPC[305]), but the judge has no obligation to give reasons for his or her decision, according to the Court of Cassation.[306]

Decisions authorising the interception of stored electronic correspondence using an electronic identifier must be reasoned.[307] Decisions authorising the use of a dedicated technical device or apparatus designed or appropriate to remotely intercept (1) technical connection data that enables the identification of terminal equipment or its user's subscription number, as well as data relating to the location of the ter-

---

301 Art. 77-1-2 PPC.

302 Art. 60-2 PPC.

303 Art. 99-4 PPC.

304 Arts. 100, §2, 100-1, and 706-95 PPC.

305 Art. 100, §1 PPC.

306 Court of Cassation, crim. ch., 27 September 2011, n° 11-81458, bull., 1er moyen (1st ground), available at https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000024672506&fastReqId=1759026642&fastPos=1; Court of Cassation, crim. ch., 22 October 2013, n° 13-81945, bull., 4ème moyen (4st ground), available at https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000028116516&fastReqId=451125653&fastPos=1

307 Arts. 706-95-1 and 706-95-2 PPC.

minal equipment used, and (2) correspondences sent or received by the terminal equipment, must be made in writing and must be reasoned, but they are not of a judicial nature and are therefore not subject to appeal.[308] Where the decision is issued by the district prosecutor (in case of emergency resulting from an imminent risk of evidence being damaged or an imminent risk of serious harm to persons or goods), the liberty and custody judge who delivered or confirmed the authorisation is informed without undue delay by the district prosecutor with regard to acts that have been performed under the current article and with regard to official records drawn-up pursuant to his authorisation.

Finally, where correspondence interception is performed through the national platform for judicial interception,[309] technical modalities of interrogation of concerned operators and of transmission of the information are regulated by a protocol provided for in article R. 15-33-72 PPC.[310]

bb) Remote data, voice and image capture

Provisions that are specific to remote data, image and voice capture do not particularly regulate the form of the opinion or of the request transmitted by the district prosecutor to, respectively, the investigating judge and the liberty and custody judge.

Remote data capture orders issued by the investigating judge or the liberty and custody judge must be reasoned.[311] Under penalty of nullity, they must mention the penal infringement that justifies the operation, the exact location or the comprehensive description of concerned computer systems and the duration of operations.[312]

Remote capture of confidential words and private images orders issued by the investigating judge or the liberty and custody judge must be made in writing and reasoned.[313] They must mention the penal infringement that justifies the operation, the duration of operations, and all the elements that enable the identification of the targeted private and public places.[314] However, these orders are not of a judicial nature and are not subject to appeal.[315]

---

308 Art. 706-95-6 PPC.

309 See above, Section III.B.4.a.bb.

310 Art. R. 40-45 PPC.

311 Arts. 706-102-1 and 2 PPC.

312 Art. 706-102-3 PPC.

313 Art. 706-97 PPC.

314 Art. 706-97 PPC.

315 Art. 706-97 PPC.

cc) Interception by service providers of the content of the information accessed by their users

Provisions that are specific to the interception of the content of the information accessed by users of electronic communications services do not regulate either the form of the requests made by the district prosecutor to the competent judge, or the order of this judge, or the requests made to Internet service providers, except where the request is made through the national platform for judicial interception.[316] In this case the technical modalities of interrogating the service providers concerned are regulated by a protocol provided for in article R. 15-33-72 PPC.[317] This protocol clarifies *inter alia* the computing systems likely to be concerned by a requisition and the nature of data that can be requested.[318]

Requests to make the intercepted information available are also subject to this protocol, as well as to a procedure described in articles R. 15-33-67 to R. 15-33-75 PPC, whether they are made through the national platform for judicial interception or not. According to this procedure, requests for making information available must be the subject of an official record indicating the recipient of the request and the nature of requested information,[319] and mentioning where needed the previous agreement of the district prosecutor, which can be granted by any means.[320]

7. Substantive prerequisites of interception orders

Substantive prerequisites of interception orders may differ according to the procedure in relation to predicate offences, but are fairly homogeneous in relation to the degree of suspicion required in relation to persons and connection under surveillance, and in relation to proportionality and possible consent given by a communication participant.

a) Degree of suspicion

Provisions that authorise the recourse to data interception do not specify a required degree of suspicion for a past crime or future danger or risk, but require that the measure is necessitated by the requirements of an investigation that fulfils the other criteria laid down by the Penal Procedure Code in relation to each particular measure.

---

316 Arts. R. 40-42 to R. 40-56 PPC. On this platform, see above, Section III.B.4.a.bb.

317 Art. R. 40-45 PPC.

318 Art. R. 13-33-72 PPC.

319 Art. R. 13-33-71 PPC.

320 Art. R. 13-33-71 PPC.

b) Predicate offences

Correspondence interception under articles 100 *et seq.* PPC may only be authorised within the framework of a judicial information targeting felonies and misdemeanours where the penalty incurred is equal to or in excess of two years' imprisonment, in addition to some specific situations such as the search for causes of death or disappearance or the non-respect of a prohibition laid down in a past sentence.[321]

Correspondence interception under article 706-95 PPC may be authorised within the framework of preliminary and flagrancy investigations, but solely in relation to an infringement considered to be organised crime or delinquency and being as such one of the misdemeanours and felonies listed in articles 706-73 and 706-73-1 PPC.[322] However, other provisions of the Penal Procedure Code may provide for the application of these special powers within the framework of other penal infringements. For example, article 706-72[323] provides for the application of articles 706-95 to 706-103 and 706-105 within the framework of investigations related to data automated processing systems violations such as unauthorised access to such systems. As another example, article 706-24-2[324] provides for the application of articles 706-95, 706-95-1, 706-95-4, 706-96, and 706-102-1 within the framework of investigations relating to offences of terrorism listed in article 706-16 PPC, where they are carried out by certain judicial police services.

For the rest, interception by service providers of the content of the information accessed by their users may be ordered in case of any penal infringement that justifies one of the three forms of judicial investigation set out under French law (flagrancy investigation, preliminary investigation or investigation procedure conducted by an investigating judge).

c) Persons and connections under surveillance and principle of subsidiarity

Interceptions of correspondence and other types of communications must be necessary to the investigation. In case of correspondence interception for the needs of a judicial information, only the information useful to ascertain the truth is transcribed.[325] This rule is also applicable within the framework of correspondence interception on the network or at the level of terminal equipment for the purpose of

---

321 See above, Section III.B.6.a.

322 These lists contain more than 30 infringements, which can be found exhaustively in the Appendix, Section B.2.

323 Modified by Law n° 2016-731 of 3 June 2016, JORF n°0129 of 4 June 2016, text n° 1.

324 Modified by Law n° 2017-1510 of 30 October 2017, JORF n° 0255 of 31 October 2017, text n° 1.

325 Art. 100-5 PPC.

organised crime repression,[326] as well as within the framework of remote capture of both data[327] and confidential words and private images.[328]

In addition, in all the procedures implemented for the purpose of organised crime and delinquency repression, interception operations may only pursue the aim of research and establishment of the penal infringements referred to in the decision,[329] sometimes under the penalty of nullity.[330]

Within the limits explained above (no other particular limits being clarified in the provisions that regulate the interception of the content of the information accessed by users[331]), the Penal Procedure Code does not specify the persons (such as suspects, intermediaries, or communication partners) who can be placed under surveillance. Nor does it require that less intrusive means be first considered or tried.

d) Proportionality of interceptions in individual cases

The prerequisites mentioned in the previous Sections are supposed to ensure proportionality of the measures to the seriousness of the offence, even though this proportionality remains relative, as previously explained in the current report,[332] since most provisions[333] clarify that "the fact that these operations reveal infringements other than those referred to in the decisions does not constitute a cause for nullity of incidental proceedings," which must be read in conjunction with article 40 PPC which commands any public agent to report any crime or misdemeanour discovered upon exercising his or her powers, along with related information, to the district prosecutor.[334]

There is no additional specific obligation, for the authorising authority, to verify that the interception is proportionate to the seriousness of the offence in the indi-

---

326 Art. 100-5 PPC being applicable according to arts. 706-95, 706-95-4, and 706-95-5 PPC.

327 Art. 706-102-8 PPC.

328 Art. 706-101 PPC.

329 Arts. 706-95-3, 706-95-7, 706-102-4, 706-96, §2, and 706-96-1, §2 PPC.

330 In all situations but remote capture of confidential words and private images: arts. 706-95-3, 706-95-7 and 706-102-4 PPC

331 Arts. 60-2, §2, 77-1-2, §2, and 99-4, § 2 PPC.

332 See Sections II.A.3., III.B.2.b.aa., and 3.b.

333 Art. 706-95-3 PPC related to access to mailboxes using a password, art. 706-95-7 related to correspondence interception at the level of terminal equipment, art. 706-102-4, §2 related to data capture, and art. 706-98-1 related to the capture of confidential words and private images.

334 Art. 40 PPC: "every constituted authority, every public officer or civil servant who, in the performance of his duties, has gained knowledge of the existence of a felony or of a misdemeanour is obliged to notify forthwith the district prosecutor of the offence and to transmit to this prosecutor any relevant information, official reports or documents."

vidual case, beyond the general principle of necessity and proportionality that judges are supposed to enforce.

e) Consent by a communication participant to the measure

The Penal Procedure Code does not provide for exceptions where a communication participant consents to the measure.

8. Validity of interception orders

Conditions for the validity of interception orders differ depending on the procedure that is followed.

a) Correspondence interception

aa) Maximum length of interception order

Correspondence interceptions ordered by the investigating judge within the framework of a judicial information,[335] and by a judge responsible for enforcing sentences within the framework of the non-respect by a condemned person (for an offence which is sentenced by two years' imprisonment or more) of the obligation to not visit certain places or persons,[336] must have a maximum duration of four months. The measure may be extended by following the same conditions as to form and duration. The Penal Procedure Code does not provide for a maximum of possible renewals but from 2016[337] the total duration cannot exceed one year or, where the offence is listed as organised crime or delinquency in articles 706-73 or 706-73-1 PPC,[338] two years.

Correspondence interceptions ordered by the investigating judge within the framework of the search of the causes of death or disappearance must have a maximum duration of two months, but they are renewable (with the one or two year limits described above also being applicable).[339]

Correspondence interceptions ordered by the liberty and custody judge of the district Court must have:

– A maximum duration of two months in the case of a search for an escaping person.[340] In this situation, the measure may be extended by following the same

---

335 Arts. 100 *et seq*. PPC

336 Art. 709-1-3 PPC.

337 Art. 100-2 PPC, modified by Law n° 2016-731 of 3 June 2016, art. 57.

338 See Appendix, Section B.2.

339 Art. 80-4 PPC.

340 Art. 74-2 PPC.

conditions as to form and duration, with a maximum duration of six months regarding misdemeanour (and with no limits regarding crimes).

– A maximum duration of one month in case of a flagrancy investigation or a preliminary investigation in relation to the restricted list of penal infringements considered being organised crime or delinquency.[341] In this situation, the measure may be extended only once by following the same conditions as to form and duration.

Correspondence interceptions at the level of terminal equipment ordered by the liberty and custody judge or the investigating judge must have a maximum duration of 48 hours. It is renewable once under the same conditions.[342]

Finally, the length of the measure consisting in accessing to a mailbox using its password is not regulated.

bb) Revocation of authorisations

In all situations, any correspondence which is useful for the discovery of the truth is transcribed and the purpose of both access to correspondence in a mailbox using its password and correspondence interception at the level of terminal equipment must be limited to the search and identification of penal infringements mentioned in the judicial authorisation, under penalty of nullity.[343.]

However, the fact that these operations reveal other penal infringements not mentioned in the judge's decision is not a cause for halting the interception, nor a cause for nullity of incidental proceedings. On the contrary, article 40 PPC permits the opening of incidental proceedings in such cases.[344]

For the rest, the Penal Procedure Code is silent on the possibility of the competent judge revoking his interception authorisation.

b) Remote data, voice and image capture

aa) Maximum length of interception order

Remote data capture orders must have a maximum duration:

– of one month where they are issued by the liberty and custody judge, renewable once under the same conditions,

– of four months where they are issued by the investigating judge, renewable under the same conditions, within a total duration not exceeding two years.[345]

---

341 See Appendix, Section B.2.

342 Arts. 706-95-4 and 706-95-5 PPC.

343 Arts. 706-95-3 and 706-95-7 PPC.

344 See above, Section III.B.7.d.

345 Art. 706-102-3 PPC.

Remote private images and confidential words capture orders must have a maximum duration:

– of one month where they are issued by the liberty and custody judge, renewable once under the same conditions,
– of two months where they are issued by the investigating judge, renewable under the same conditions, within a total duration not exceeding two years.[346]

bb) Revocation of authorisations

In all situations, only the data that is needed to ascertain the truth is described or transcribed, in an official record filed in the criminal case file, and no sequence relating to private life which has no relation with penal infringements mentioned in the authorisation can be kept in the criminal case file.[347]

Regarding remote data capture only, the Penal Procedure Code clarifies that the purpose of operations must be limited to the investigation and identification of penal infringements mentioned in the authorisation of the judge who ordered it, under penalty of nullity.[348.]

However, in all cases, the fact that these operations reveal other penal infringements not mentioned in the judge's decision is neither a cause for halting the interception, nor a cause for nullity of incidental proceedings.[349] On the contrary, article 40 PPC allows the opening of incidental proceedings in such case.[350]

However, the judge who ordered the measure may, at any time, require the interruption of data capture operations (the Penal Procedure Code being silent in relation to image and word capture).[351]

c) Interception by service providers of the content of the information accessed by their users

aa) Maximum length of interception order

The preservation of the text of the information consulted by persons using the services provided by the operators must not exceed one year.[352]

---

346 Art. 706-98 PPC.
347 Arts. 706-102-8 and 706-101 PPC .
348 Art. 706-102-4 PPC.
349 Arts. 706-98-1 and 706-102-4 PPC.
350 See above, Section III.B.7.d.
351 Art. 706-102-4 PPC.
352 Art. 60-2 PPC.

bb) Revocation of authorisations

The Penal Procedure Code does not set out particular conditions regarding the specification, in the preservation authorisation and request, of the offence that justifies the request for information preservation. The Penal Procedure Code is also silent on the possibility for the competent authority to revoke his authorisation.

9. Duties to record, report, and destroy

Duties to record, report, and destroy differ depending on the procedure that is followed.

a) Correspondence interception

In all cases, interception operations, including through the access to a mailbox using its password, are performed under the authority and supervision of the judge who ordered them.[353]

Where correspondence interception is performed through the national platform for judicial interception,[354] data relating to electronic communications being the object of an interception is placed under seal within the data processing unit until the expiry of the limitation period for prosecution. Any operation relating to the processing is registered, along with the identification of the user, the date, the time, and the nature of the operation, for a five-year period.[355]

Where the recourse to the national platform for interception is not provided for by law[356] or not technically possible, the following rules apply:

Concerning interception of correspondences on the network and at the level of terminal equipment, each interception and recording operation must be the object of the drafting of an official record, which must mention the date and time when the operation started and ended.[357] Recordings are placed under closed official seals.[358] An official record is also made of any correspondence transcription, and attached to the case file.[359] In relation to correspondence interceptions on the network, the Penal Procedure Code adds that reports of operations are addressed to the judge who authorised them.[360] In relation to correspondence interception at the lev-

---

353 Arts. 100-1, 706-95, 706-95-3, 706-95-7 PPC.

354 See above, Section III.B.4.a.bb.

355 Art. R. 40-50 PPC.

356 See above, Section III.B.4.a.bb.

357 Arts. 100-4 and 706-95-9 PPC.

358 Art. 100-4 PPC (applicable within the framework of the other procedure).

359 Art. 100-5 PPC (applicable within the framework of the other procedure).

360 Arts. 100, 74-2, and 706-95 PPC.

el of terminal equipment authorised within the framework of a preliminary or a flagrancy investigation relating to organised crime, the Penal Procedure Code adds that the liberty and custody judge who delivered or confirmed the authorisation is informed without undue delay by the district prosecutor about acts that have been accomplished and of official records that have been established as a result of their authorisation.[361]

Recordings are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution. An official record is made of the destruction.[362]

Concerning correspondence and stored correspondence that would be intercepted through the access to a mailbox using a password, this can be seized and registered or copied on any support.[363] Provisions regulating this power are silent in relation to the destruction of seized information, which implies the application of the rule established in relation to seizures in general.[364]

b) Remote data, voice and image capture

Interception operations are performed under the authority and supervision of the judge who ordered them.[365]

The investigating judge, the district prosecutor, or the appointed judicial police officer must draft an official record of each of the operations aiming at implementing the technical device that enables data capture and of the data capture operations themselves. This official record must mention the date and time when the operation started and ended. Recordings are placed under closed official seals.[366] The same persons must also describe or transcribe, in an official record attached to the case file, data or images or words (depending on the exact procedure) that are useful to ascertain the truth. Conversations in foreign language are transcribed with the assistance of a translator who is required to this end.[367]

In relation to data capture during preliminary and flagrancy investigations only, the Penal Procedure Code adds that the liberty and custody judge who authorised operations is informed without undue delay by the district prosecutor about acts that have been accomplished and of official records that have been established as a result of their authorisation.[368]

---

361 Art. 706-95-4 PPC.
362 Arts. 100-6 and 706-95-10 PPC.
363 Arts. 706-95-1 and 706-95-2 PPC.
364 Arts. 41-4, 56 and 57-1 PPC.
365 Arts. 706-102-4 and 706-98-1 PPC.
366 Arts. 706-102-7 and 706-100 PPC.
367 Arts. 706-101 and 706-102-8 PPC.
368 Art. 706-101-1 PPC.

In all situations, recordings are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution. An official record is made of the destruction.[369]

c) Interception by service providers of the content of the information accessed by their users

Where it is technically feasible, requests for preservation of the content and requests to access this information are transmitted through the national platform for judicial interception.[370] Within this context, collected data, as well as information relating to voice recognition, is kept until the investigation is closed by the judicial police officer and the proceeding are transmitted to the competent judicial authority.[371] Any operation relating to the processing is registered, along with the identification of the user, the date, the time, and the nature of the operation, for a five-year period.[372] In addition, the protocol provided for in article R. 15-33-72 PPC[373] applies.[374] This protocol, which must be communicated to the French data protection authority by requested persons on the occasion of other formalities they must fulfil under the data protection law,[375] clarifies *inter alia* the modalities for consultation of the information, conditions for security of the information in the course of its transfer to the demanding judge or police officer, modalities for tracking requests and visualisation, and guarantees that enable to limit the access to requested information only and to prevent access to information protected by a secret falling within the scope of the law (including medical secrecy), at the exclusion of cases where law provides that this secret is not binding on the judicial authority.[376]

The protocol under article R. 15-33-72 PPC is also applicable where the national platform for interception is not used.

In all case of requests to access information intercepted by service providers in relation to information accessed online, the procedure described in articles R. 15-33-67 to R. 15-33-75 PC is also applicable. According to these provisions, receipt of information must be the subject of an official record (which can be the same as the one established where the information is requested[377]), and this information is either printed on a paper, or entirely safeguarded on a digital support in compliance

---

369 Arts. 706-102 and 706-102-9 PPC.

370 See above, Section III.B.4.a.bb.

371 Art. R. 40-49 PPC.

372 Art. R. 40-50 PPC.

373 See above, Section III.B.6.b.cc.

374 Art. R. 40-45 PPC.

375 Art. R. 13-33-73 PPC.

376 Art. R. 13-33-72 PPC.

377 See above, Section III.B.6.b.cc.

with technical standards that are applicable at the moment of the transmission.[378] This paper document or this digital support is attached to the official record and in case a digital support has been created, a copy of it is placed under closed seals.[379]

However, in the above-mentioned provisions, as well as in other provisions relating to the above-mentioned type of interceptions, the destruction of recordings is not provided for where the national platform for judicial interceptions is not used. The regime that surrounds seizures and requisitions is therefore applicable.[380]

10. Notification duties, remedies, and consequences

Procedural efficiency implies the secrecy of interception measures.[381] Therefore, the accused can only have knowledge of their existence and results at the moment he is granted access to the entire procedural case file, this moment being determined by the Penal Procedure Code, depending on the nature of the procedure.[382]

Procedural acts resulting from these measures can be annulled, especially where a substantive requirement laid down in the Penal Procedure Code which has affected the interests of the concerned party has not been respected,[383] or where it is provided in the provision of the Penal Procedure Code related to the concerned measure.[384] For example, as we analysed it, the penalty of nullity is the consequence of a correspondence interception that takes place without respecting the requirements surrounding the implementation of such a measure on the line of a protected person (such as advocates or journalists) mentioned in articles 100-5 and 100-7 PPC.

11. Confidentiality requirements

Any person who provides support to the investigation must keep his or her support measure confidential, including Internet service providers. Any violation of this obligation of professional secrecy may incur a penal sanction under articles 226-13 and 226-14 PPC.[385]

---

[378] Art. R. 13-33-74 PPC.

[379] Art. R. 13-33-74 PPC.

[380] Arts. 41-4, 56, and 57-1 PPC.

[381] See, e.g., Jacques Beaume, *Rapport sur la procédure* pénale, July 2014, p. 43 available at http://www.justice.gouv.fr/publication/rap-beaume-2014.pdf

[382] See mainly arts. 393, 278, and 279 PPC.

[383] Even where the Penal Procedure Code states explicitly that the non-respect of a given requirement is not a cause for nullity, this statement may be challenged based on the provisions of the European Convention of Human Rights or based on constitutional provisions (through, in this latter case, a "priority request" from the Court of Cassation to the Constitutional Council).

[384] See mainly arts. 170, 171, and 385 PPC.

[385] Art. 11 PPC.

C. Collection and Retention of Traffic Data and Subscriber Data

French law does provide for the possibility for the judicial authority to collect traffic and subscriber data and, in certain circumstances, to intercept such data, both including geolocation data.

1. Collection of traffic data and subscriber data

a) Judicial requisition of traffic and subscriber data

aa) Relevant provisions

(1) Requisition of subscribers' and traffic data including location data

Traffic and connection data retained by access and hosting service providers[386] can be requisitioned in case of any penal infringement that justifies one of the three forms of judicial investigation set out under French law. The requisition is made by the district prosecutor or by a judicial police officer upon authorisation of the district prosecutor within the framework of preliminary investigations,[387] by the district prosecutor or by a judicial police officer within the framework of flagrancy investigations,[388] and by the investigating judge or the judicial police officer appointed by him within the framework of judicial investigation.[389] These traffic and connection data may be acquired by electronic or telematic means.[390]

Requisition of data by any means

Article 60-1

The district prosecutor or a judicial police officer may, by any means, order any person, establishment or organisation, whether public or private, or any public services likely to possess any documents relevant to the inquiry in progress, including those produced from a computer system or a personal data processing system, to provide them with these documents, including in digital format. Without legitimate grounds, the duty of professional secrecy may not be given as a reason for non-compliance. […]

[…], failure to respond to such an order as quickly as possible is punished by a fine of €3570. […]

Article 77-1-1

The district prosecutor or on his authorisation a judicial police officer, may, by any means, order any person, establishment or organisation, whether public or private, or any public services liable to possess any documents relevant to the inquiry in progress,

---

386 On the basis of art. L. 34-1 PECC and of art. 6 of the Law n° 2004-575 of 21 June 2004 regarding confidence in the digital economy (called "LCEN"). See below, Section b.

387 Art. 77-1-1 PPC.

388 Art. 60-1 PPC.

389 Art. 99-3 PPC.

390 Arts. 77-1-2, 60-2, and 99-4 PPC.

including those produced from a computer system or a personal data processing system, to provide them with these documents, including in digital format. Without legitimate grounds, the duty of professional secrecy cannot be given as a reason for non-compliance with this order. […]

Where there is no response to these orders, the provisions of the second paragraph of article 60-1 are applicable. […]

Article 99-3

An investigating judge or judicial police officer delegated by him may, by any means, order any person, establishment or organisation, whether public or private, or any public services liable to possess any documents relevant to the investigation, including those produced from a computer system or a personal data processing system, to provide them with these documents, including in digital format. Without legitimate grounds, the duty of professional secrecy may not be given as a reason for non-compliance with such an order. […]

Where the person does not respond to this order, the provisions of the second paragraph of article 60-1 are applicable.

[…]

Requisition of data by any electronic or telematic means

Article 60-2, §1

At the request of a judicial police officer, who can intervene by means of telecommunications or computers, public organisations or private legal persons, with the exception of those set out in the second paragraph of article 8, II, 3° and in article 67, 2° of Law no. 78-17 of 6 January 1978 relating to computers, databases, and liberties,[391] must make available information helpful for the discovery of the truth, with the exception of information the secrecy of which is protected by statute, where it is stored in one or more computer or data processing systems that they administer.

Article 60-2, §5

A Decree of the Council of State made on the advice of the National Commission for Data Protection determines the categories of organisation covered by the first paragraph, and also the methods for examining, transmitting and processing the required information.[392]

Article 77-1-2, §1

On the authorisation of the district prosecutor, a judicial police officer may carry out the measures provided for in the first paragraph of article 60-2.

Article 99-4, §1

Where necessary to carry out a rogatory commission, a judicial police officer may issue the demands provided for in the first paragraph of article 60-2.

---

391 These persons are the members of a non-profit association or entity of a philosophical, political, religious or trade-union character, the persons who have regular contacts with such association or entity within the framework of its activities (art. 8, II, 3°, §2 of Law n° 78-17), and professional journalists (art. 67, 2° of Law n° 78-17).

392 Decree n° 2008-150 of 19 February 2008, creating arts. R. 15-33-67 to R. 15-33-75 PPC.

(2) Access to subscribers lists

Provisions mentioned above also enable to access subscribers lists. In addition, article L. 33-1, V PECC requires electronic communications operators to enable access by the judiciary, the national police, the national gendarmerie, fire and rescue services, and emergency services, when these services act within the framework of their respective judicial or rescue missions, to the comprehensive, unredacted, and updated list of their users and subscribers.

bb) Formal and substantial prerequisite and procedure of disclosure

The Penal Procedure Code does not provide for specific prerequisite in relation to the form or the content of requisitions and of answers that are not made by telematic or electronic means, which must follow the general rules of the penal procedure.

Electronic and telematic requisitions and answers to these requisitions on the basis of the first § of articles 60-2, 77-1-2 and 99-4 PPC are for their part regulated in articles R. 15-33-67 to R. 15-33-75 PPC, which content has already been presented previously in this report.[393]

In addition, these same requisitions,[394] which might serve to request traffic and subscribers data, must be issued through the national platform for judicial interceptions, regulated in articles R. 40-42 to R. 40-56 PPC, unless it is technically not feasible.[395] The procedure to be followed in this case has also already been presented previously in this report.[396] Substantial prerequisite are not different from Section 7 of the current report in relation to requests for interception of the content of the information consulted by users.

cc) Duty of addressees to disclose information

Duty of addressees to cooperate in this context is regulated by general provisions on the duty of electronic communications service providers – and more widely the duty of any citizen – to provide support to justice for the manifestation of the truth.[397]

In addition, Internet access service providers and hosting providers who do not retain connection data according to article 6 of the Law n° 2004-275, or do not answer a communication request form the judiciary, may be punished by one year imprisonment and a fine of €75,000. Legal persons may be penally liable and

393 See above, Sections III.B.6.b.cc. and III.B.9.c.

394 Regulated by arts. 60-2, 77-1-2 and 99-4 PPC.

395 Art. 230-45 PPC.

396 See above, Sections III.B.6.b.cc. and 9.c.

397 See above, Section III.B.5.

amongst possible penalties lies the prohibition to exercise for a maximum of five years the professional activity in the course of which the infringement has been committed.[398]

Electronic communications operators and Internet access service providers who do not retain traffic data within the conditions laid down by law (including not anonymising these data when required by law) may be punished by one year imprisonment and a fine of €75,000. Legal persons may be penally liable and amongst possible penalties lies the prohibition to exercise for five years the professional activity in the course of which the infringement has been committed.[399]

Finally, non-disclosure without undue delay to a requisition under article 60-1 PPC is punished by a fine of €3750. This concerns equivalently requisitions of traffic data and requisitions of users and subscribers lists.

b) Data retention

The obligations of Internet services providers to retain traffic and connection data are laid down in article L. 34-1 PECC (retention of traffic data by operators and Internet access providers) and article 6, II of the Law n° 2004-575 (retention of connection data by Internet access providers and hosting providers).[400]

Data to be retained are specified in two decrees:

– Decree n° 2006-358 of 24 March 2004, which created articles R. 10-12 *et seq.* PECC, issued in application of article L. 34-1 of the same Code, articles which have been later modified;[401]
– Decree n° 2011-219 of 25 February 2011 modified,[402] issued under article 6 of Law n° 2004-575.

As a result, traffic data to be retained (for a duration of one year) under article L. 34-1 PECC, in order to identify and prosecute penal infringements, according to article R. 10-13 of the same Code, are the following technical data:

– information enabling the identification of the user;
– data relating to terminal communication equipment used;
– technical specifications and date, time, and duration of each communication;

---

398 Art. 6, VI of Law n° 2004-575 of 21 June 2004 regarding confidence in the digital economy (called "LCEN").

399 Art. L. 39-3 PECC.

400 Law n° 2004-575 of 21 June 2004 regarding confidence in the digital economy (called "LCEN").

401 Decree n° 2012-436 of 30 March 2012 (art. 7), Decree n° 2015-349 of 27 March 2015 (art. 3) and Decree n° 2008-1136 of 13 December 2018 (art. 2).

402 Decree n°2012-436 of 30 March 2012 (art. 28) and Decree n° 2014-1576 of 24 December 2014 (art. 2).

– data relating to complementary services requested or used and their providers;
– data enabling the identification the recipients of the communication.

In addition to these data, for telephony activities, the operator must retain data that enable the identification of the origin and the location of the communication.

Connection data to be retained (for a duration of one year) under article 6 of Law n° 2004-575 according to Decree n° 2011-219, are once again only technical data, excluding other types of information (such as names, passwords, etc.) if such data are not usually collected. These data include – notably – the following:
– the identifier of the connection;
– the identifier attributed to the subscriber;
– the identifier of the terminal used for the purpose of the connection, when providers access such information;
– the dates and times at which the connection begins and ends;
– the specifications of the line of the subscriber;
– certain information provided at the time of the contract subscription or of the creation of the users' account, including – only where the provider usually collects such information – the password and the data that enables the modification or verification of this password, in their latest and updated form.

2. Interception of subscribers' and traffic data including location data

French law enables real-time geolocation, as well as the interception of connexion and subscribers' data at the level of terminal equipment.

a) Real-time geolocation

Real-time geolocation of a person, a vehicle or an object, without the consent of this person or the owner of this vehicle or object, can be done in limited situations (investigation related to a felony or misdemeanour sentenced at least by five years of imprisonment, or related to an escape from detention or to the provision of assistance to the author of a terrorism act, or related to a death, a disappearance or an escape[403]) according to articles 230-32 to 230-44 PPC.

The measure is authorised, in writing,[404] by the investigating judge in case of judicial information relating to the determination of the cause of death or disappearance (for a maximal duration of four months renewable under the same conditions of form and duration) and by the district prosecutor in other situations (for a maximal duration of 15 consecutive days, which may be followed by a measure of the

---

403 Art. 230-32 PPC.

404 Art. 230-33 PPC. This decision is, however, not a jurisdictional decision and it cannot be appealed (same provision).

same nature, authorised by the liberty and custody judge at the request of the district prosecutor, for a maximal duration of one month renewable under the same conditions of form and duration).[405]

The measure is implemented under the supervision of the magistrate who authorised them or their prolongation,[406] by a judicial police officer or, under his or her responsibility, a judicial police agent, or it is prescribed by the judicial police officer.[407] It may be implemented on the whole French territory through the use of any means,[408] and the competent magistrate or judicial police officer may request the assistance of any qualified agent belonging to a service or unit or body placed under the authority or supervision of the Ministry of the Interior and of which a list is determined by means of a decree, in order to implement and remove the technical device that enables geolocation.[409]

If the needs of the investigation call for it, the investigating judge or the district prosecutor may authorise in writing the intrusion in a private place or a vehicle, on the sole purpose to implement a geolocation device, including outside the visit times established in article 59 PPC in relation to searches and houses visit.[410] Where this private place is not used or dedicated to the storage of goods, this possibility is, however, restricted to particular investigations (search for the causes of death or disappearance, escape or investigation relating to a penal infringement sentenced at least by five years' imprisonment). Where this private place is a home, the written authorisation must be provided by the liberty and custody judge or the investigating judge, depending on certain circumstances described in article 230-34 PPC.

Such intrusion may in addition be performed upon decision of a judicial police officer where there is an imminent risk targeting the integrity of evidence or an imminent risk of serious harm to people or goods. This police officer must in this situation inform immediately, by any means, the competent magistrate, who may order the release of geolocation. If the intrusion in a home is necessary, this magistrate must before the implementation of the measure give his or her agreement, by any means, and confirm it in writing within a delay of 24 hours, otherwise the geolocation is stopped.[411]

---

405 Art. 230-33 PPC.

406 Art. 230-37 PPC.

407 Art. 230-32 PPC.

408 Art. 230-32 PPC.

409 Art. 230-36 PPC.

410 Art. 230-34 PPC. Art. 59 states that, except where they are requested from within a building or in the exceptional cases provided for by law, searches and house visits may not be undertaken before 6 am or after 9 pm.

411 Art. 230-35 PPC.

All operations are the subject of official records, mentioning the date and time at which operations began and ended, recordings are placed under closed seals,[412] and information useful to ascertain the truth is transcribed in an official record by the competent judicial police officer or agent.[413]

The Penal Procedure Code also provides for the possibility to not mention in the case file certain elements such as the time and date of operations, the location records and the identity of a person having providing assistance in order to implement the geolocation device, under particular circumstances linked to organised crime or delinquency and following a specific procedure.[414] The Code also provides for the possibility to contest the recourse to geolocation, which might be annulled under particular conditions.[415]

Recordings are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution. An official record is made of the destruction.[416]

Finally, the Penal Procedure Code clarifies that this procedure that enables geolocation is not applicable were real-time geolocation operations aim at locating in real time an electronic communication terminal equipment, a vehicle or an object whose owner or legitimate possessor is the victim of the penal infringement that justifies the investigation or a disappeared person, on the sole purpose of locating this person or the object that has been stolen from him or her. In such situation, real-time geolocation operations are the object of requisitions under articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3 or 99-4[417] PPC.[418]

b) Interception of connexion data and subscribers data at the level of terminal equipments

Articles 706-95-4 and 706-95-5 PPC grant the investigating judge and the liberty and custody judge with the power to authorise, for the purpose of the repression of organised crime, the capture of technical connection data that enable to identify a terminal equipment or its user's subscription number, as well as data related to the location of the terminal equipment used. This remote capture is performed through the use of a "technical device" which must be understood, within the framework of

---

412 Art. 230-38 PPC.

413 Art. 230-39 PPC.

414 Art. 230-40 PPC. See also art. 230-42 PPC.

415 Art. 230-41 PPC.

416 Art. 230-43 PPC.

417 See above, Section III.C.1.

418 Art. 230-44 PPC.

this procedure, as any "hardware or software,"[419] but which primarily refers, in the legislator's intent, to "proximity technical device" (also called IMSI catcher).[420]

Since this procedure also enables to intercept correspondences sent or received by this terminal equipment, the modalities of execution of orders, the formal and substantial prerequisite of the latter, the duties to record, report, and destroy and – where technically feasible and provided for by Decree of the Council of State – the necessity to implement the measure by using the national platform for judicial interception, have already been explained previously in the current report in dedicated Sections.

The sole difference lies in the maximum duration of the measure, which is:

– of one month where they are issued by the liberty and custody judge, renewable one single time under the same conditions,
– of two months where they are issued by the investigating judge, renewable under the same conditions, within a total duration not exceeding six months.[421]

D. Access to Stored Communication Data

Access to stored communication data may mainly be performed through requisitions, search and seizure and online search with the help of remote forensic software.

1. Judicial requisitions

During investigations, the district prosecutor, a judicial police officer (upon authorisation of the district prosecutor in case of preliminary investigation) or the investigating judge, have the following powers:

– to request from any person or organism, of a private or a public nature, where the latter are likely to detain information that can be of interest for the investigation, to provide this information, including through electronic means;[422]

---

[419] Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal [Administrative decision determining the list of apparatuses and technical devices, provided for in article 226-3 PC], Annex 1, modified, available at https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=6BB0AE272B2AC4D0F771ED8BAE7E76E9.tplgfr38s_1?idArticle=LEGIARTI000033064127&cidTexte=JORFTEXT000026241910&categorieLien=id&dateTexte=20160930. Indeed, arts. 706-95-4 and 706-95-5 provide for the use of apparatuses or devices described in art. 226-3 PC in order to intercept communications, the use of these apparatuses and devices being prohibited outside the framework of authorised judicial or administrative interceptions.

[420] See above, Section III.B.4.a.aa.

[421] Arts. 706-95-4 and 706-95-5 PPC.

[422] Arts. 60-1, 77-1-1, and 99-3 PPC.

– to request electronically, from all legal persons of a private or public nature at the exception of a list of protected persons,[423] information useful to ascertain the truth, at the exception of secrets protected by law, that are stored in computing systems.[424]

The procedures to be followed are the same as the ones that can be used in order to request traffic and subscribers data from electronic communication operators.[425]

2. Search and seizure of stored electronic communication data

The search and seizure procedure is applicable to stored electronic communication data. A duty to cooperate is set out, and non-cooperation is punished by the Penal Code. This duty to cooperate is also currently applicable to the defendant, who risks an increase of the sentence if they are found guilty.

a) Applicability of seizure provisions to electronic data

Search and seizure of information held by a third party is set out in articles 76 to 76-3 (preliminary investigation), 56 to 59 (flagrancy investigation), 92 to 99-4 (investigation procedure conducted by an investigative judge), and 706-89 (in relation with a limited list of crime or misdemeanours) PPC.

This general procedure, performed by a judicial police officer or an investigating judge,[426] is applicable to stored electronic communication data, in computer systems that lie on the places that are searched, in computer systems that are connected to these latter systems, and in computer systems that are connected to systems located at the police services premises. Indeed, the Penal Procedure Code[427] states that judicial police officers and agents may, during a search performed in compliance with this Code, access, through a computer system that is on the place that is searched, to data that are of interest for the investigation and that are stored in this computer system or in another computer system, as long as these data are accessi-

---

[423] Protected persons are those mentioned in art. 8, II, 3° §2 (non-profit associations or organisms of a religious, philosophical, political or union nature, in relation, only, to sensitive data corresponding to the object of the concerned association or organism) and in art. 67, 2° of Law n° 78-17 modified on the protection of personal data (organisms that process personal data for the sole purpose of the professional exercise of an activity of journalism respecting deontological rules of this profession).

[424] Arts. 60-2, §1, 77-1-2, §1, and 99-4, §1 PPC.

[425] See above, Section III.C.1.a. Arts. 60-2, §2, 77-1-2, §2, and 99-4, §2 PPC. See above, Section III.B.1.g.

[426] Arts. 56, 76, and 94 *et seq*. PPC.

[427] Art. 57-1 PPC (relating to flagrancy investigations). See also (for the application of the same rules within the framework of preliminary investigations and judicial information) arts. 76-3, 97, and 97-1 PPC.

ble from or for the initial system.[428] They may also, in compliance with rules governing search, access through a computer system that is on the premises of a unit or a service of the Police or of the Gendarmerie, to data that are of interest for the investigation and that are stored in another computer system, as long as these data are accessible from the initial system.[429] Where it is beforehand established that these data, accessible from or for the initial system, are stored in a computer system that is located outside the national territory, they are collected subject to conditions of access under applicable international commitments.[430] Collected data may be copied on any support, and digital supports may be seized and placed under seals under the conditions set out by the Penal Procedure Code.[431]

As already explained previously in this report, this procedure may also be used in order to access correspondence before and after their transmission.[432]

Safeguards and requirements are different from those surrounding the interception of correspondence and remote access to data, since the privacy limitation is in this case considered lower. For example, the procedure of search and seizure can be used within the framework of any investigation, and is not limited to the investigation of certain kinds of penal infringements only. Safeguards include the drafting of an official report of the search, the initiation of steps that are necessary to ensure the observance of professional secrecy and the defendant's rights, the inventory and placement under official seals of any document or article seized, a restriction of access to consulted documents and information to the police officer who carries out the search and potential qualified persons requisitioned to help him, and the presence, during search and seizure, of the person in whose domicile the search is made, or of two witnesses. In addition, certain categories of persons benefit from a higher level of protection (advocates, media companies, audio-visual communication companies, online public communication companies, press agencies, journalists, doctors, notaries, bailiffs, judges).[433]

b) Duties to cooperate: production and decryption orders

During search and seizure, judicial police officers (or, under their responsibility, judicial police agents) may, by any means, require any person who may be aware of the security measures applied in order to protect the data that can be accessed during the search, or who may supply them with the information that is necessary to access to these data. Failure to respond to this request at the earliest opportunity

428 Art. 57-1, §1 PPC.
429 Art. 57-1, §2 PPC.
430 Art. 57-1, §3 PPC.
431 Art. 57-1, §4 PPC.
432 See above, Section III.B.2.b.
433 Arts. 56-1 to 56-5 PPC.

is punishable by a fine of €3750, except for some particularly protected people to whom such a sanction does not apply (advocates, media companies, audio-visual communication companies, online public communication companies, press agencies, journalists, doctors, notaries, bailiffs).[434]

In addition, the Penal Code punishes some refusals to cooperate.

> **Article 434-15-2** (as last modified by Law n° 2001-1062)
>
> A penalty of three years' imprisonment and a fine of €270,000[435] are incurred by anyone who, having the key to decipher an encrypted message which may have been used to prepare, facilitate or commit a felony or a misdemeanour, refuses to disclose that key to the judicial authorities or to operate it following instructions issued by the judicial authorities under of title II and III of Book I of the Code of penal procedure.
>
> Where the refusal was made where the disclosure of the key or its operation would have prevented the commission of a felony or a misdemeanour or would have limited its consequences, the penalty is increased to five years' imprisonment and a fine of €450,000.

c) Application to the defendant

The duty to cooperate is not applicable to the defendant, in accordance with the principle of prohibition of self-incrimination. Similarly, in the opinion of the author, the penal infringement provided for in article 434-15-2 PC should not be applicable to the defendant for the same reason. However, despite the fact that a part of the doctrine and of practitioners agree on that issue,[436] the Constitutional Council decided, on March 2018,[437] that this penal infringement is compliant with the French Constitution and does not violate the defendants' rights where it applies to this defendant because he or she refused to communicate the password that enables to read information stored on its terminal device. Some authors consider that this issue should in the future be subject of proceedings before the European Court of Human Rights.[438]

---

434 Art. 57-1, §5 *et seq.* PPC.

435 This amount has replaced the amount of €45,000 according to Law n°2016-731 of 3 June 2016 (art. 16).

436 See, e.g., Camille Polloni, "Si la police le demande, est-on obligé de donner son mot de passe?," 5 Feb. 2015, Rue 89, available at http://rue89.nouvelobs.com/2015/02/05/si-police-demande-est-oblige-donner-mot-passe-257509. This press article includes the interview of advocates and National Gendarmerie representatives. In its decision of January 2018 in which it referred back the question to the Constitutional Council, the Court of Cassation declared itself that article 434-15-1 PC "might violate the right to not give a statement and the right against self-incrimination resulting from articles 9 and 16 of the Human and Citizens' Rights Declaration of 26 August 1789" (which has a constitutional value): Court of Cassation, crim. ch., 10 January 2018, n°17-90019, available at https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000036635139&fastReqId=307018589&fastPos=1

437 Constitutional Council, Decision n°2018-696 QPC of 30 March 2018, available at https://www.conseil-constitutionnel.fr/decision/2018/2018696QPC.htm

438 See, e.g., Eric A. Caprioli, "Sécurité, cryptologie et libertés", 18 October 2013, updated September 2002, Section III, 1, first publication in Le Bulletin du Barreau de Nice,

This being said, a defendant who refused to cooperate may be punished more severely if found guilty, on the basis of article 132-79 PC.

Article 132-79 (inserted and last modified by Law n° 2004-575)

Where a means of encryption, in the sense of article 29 of act no. 2004-575 of 21 June 2004 used to ensure confidentiality in the digital economy has been used to prepare or commit a felony or a misdemeanour, or to facilitate the preparation of commission of a felony or a misdemeanour, the maximum prison sentence incurred is raised as follows:

1° where the offence is punished by thirty years' imprisonment, this is increased to life imprisonment;

2° where the offence is punished by twenty years' imprisonment, this is increased to thirty;

3° where the offence is punished by fifteen years' imprisonment, this is increased to twenty;

4° where the offence is punished by ten years' imprisonment, this is increased to fifteen;

5° where the offence is punished by seven years' imprisonment, this is increased to ten;

6° where the offence is punished by five years' imprisonment, this is increased to seven;

7° where the offence is punished by a maximum of three years' imprisonment, this is doubled.

The provisions of the present article are, however, not applicable to the perpetrator of or the accomplice to an offence who, at the request of the judicial or administrative authorities, has provided them with an unencrypted version of the coded messages and the secret keys necessary to decipher them.

d) Power of judicial authorities to decrypt encrypted data that are necessary to ascertain the truth

Articles 230-1 to 230-5 PPC provide for the possibility for judicial authorities to decrypt encrypted data that are necessary to ascertain the truth.[439]

Article 230-1 (inserted by Law no. 2001-1062 of 15 November 2001 article 30 Official Journal of 16 November 2001); (Law no. 2004-575 of 21 June 2004 article 38 Official Journal of 22 June 2004) (modified by Law n°2014-1353 of 13 November 2014)

Without prejudice to the provisions of articles 60, 77-1 and 156, where it appears that data seized or obtained during the course of the inquiry or investigation has been altered, preventing access to or understanding of the information in clear that it contains, or where it appears that these data are protected by an authentication mechanism, the district prosecutor, the investigating jurisdiction, the judicial police officer authorised by

---

September 2002, p. 10-12, available at https://www.caprioli-avocats.com/fr/informations/securite-cryptologie-et-libertes--securite-de-linformation-21-29-0.html; Caroline Piquet, *Refuser de donner son code de téléphone en garde à vue est passible de poursuites* [Refusing to provide one's phone code in custody is subject to legal action], 18 April 2018, Le Figaro.fr, http://www.lefigaro.fr/actualite-france/2018/04/18/01016-20180418ARTFIG00290-refuser-de-donner-son-code-de-telephone-en-garde-a-vue-est-passible-de-poursuites.php

439 The following articles correspond to the translation proposed by Legifrance, and modified by the author of the current report in order to take into account most recent modifications made to these articles by Law n° 2014-1353 of 13 November 2014.

the district prosecutor or by the investigating judge, or the trial court seized of the case may appoint any qualified legal or natural person to carry out the technical operations necessary to obtain access to this information, to obtain a readable version of this information, and also, where a method of encryption has been used, the secret key for decoding it, if this appears necessary.

If the person thus appointed is a legal person, his legal representative submits for the approval of the district prosecutor, the judicial police officer or the court seized of the case the name of the natural person or persons who, within this legal person and under its name, will carry out the technical operations mentioned in the first paragraph. Unless these persons are registered on a list provided for in article 157, the persons thus nominated swear the oath provided for in the second paragraph of article 60 and by article 160, in writing.

If the penalty applicable to the offence is of at least two years' imprisonment and the needs of the inquiry or investigation justify this, the district prosecutor, the investigating jurisdiction, the judicial police officer authorised by the district prosecutor or by the investigating judge, or the trial court seized of the case may order the use of means protected by National Defence secrecy, following procedures laid down by the present chapter.

Article 230-2 (inserted by Law no. 2001-1062 of 15 November 2001 article 30 Official Journal of 16 November 2001) (modified by Law n°2014-1353 of 13 November 2014 and by Law n°2018-699 of 3 August 2018)

Where the district prosecutor, the investigating court, the judicial police officer authorised by the district prosecutor or by the investigating judge, or the trial court in charge of the case decide to use, for the procedures mentioned in article 230-1, means protected by official State secrecy, the written submission must be sent to a technical organisation subject to the obligations of National Defence secrecy and designated for this purpose by Decree, along with the medium containing the data to be deciphered or a copy of it. This submission fixes the time limit in which these deciphering procedures must be carried out. The time limit may be extended under the same conditions or form. At any time, the district prosecutor, the investigating court, the judicial police officer authorised by the district prosecutor or by the investigating judge, or the trial court which is in charge of the case or which has requisitioned the technical organisation, may order the interruption of these prescribed procedures.

For purposes of performing decipherment operations, the technical organisation mentioned in the first paragraph of the current article is entitled to open or re-open judicial seals and to create new seals after having where necessary reconditioned the physical devices it had in charge to examine. In case there is a risk of destruction of data or of the physical device that contains the latter, the authorisation to alter the physical device must be delivered by the district prosecutor, the investigating court or the trial court in charge of the case.

Data protected in the interests of national security may only be passed on under the conditions provided for in articles L. 2312-4 to L. 2312-8 of the Code of Defence.

Where data concerned are data obtained within the framework of electronic communications interceptions, within the processing mentioned in I of article 230-45, the requisition order is directly addressed to the technical organisation mentioned in the first paragraph of the current article.

Article 230-3 (inserted by Law no. 2001-1062 of 15 November 2001 article 30 Official Journal of 16 November 2001) (modified by Law n°2014-1353 of 13 November 2014 and by Law n°2016-731 of 3 June 2016)

As soon as the procedures have been completed, or as soon as it becomes clear that the procedures are technically impossible, or at the expiry of the time limit prescribed, or when an interruption order is received from the district prosecutor, the investigating court, the judicial police officer authorised by the district prosecutor or by the investigating judge, or the trial court in charge of the case, the results obtained and the documents received are returned by the head of the technical organisation to the author of the requisition order or to the judge concerned where the requisition has been addressed directly by him or her. Subject to the obligations of National Defence secrecy, the results are accompanied by technical instructions enabling them to be understood and used, as well as by a statement drawn up by the head of the technical organisation, which attests to the genuineness of the results.

The facts thus obtained are recorded in an official record marking their receipt and are added to the case file of the proceedings.

Article 230-4 (inserted by Law no. 2001-1062 of 15 November 2001 article 30 Official Journal of 16 November 2001) (modified by Law n°2014-1353 of 13 November 2014)

Judicial decisions taken pursuant to the present chapter do not have judicial status and are not subject to appeal.

Article 230-5 (inserted by Law no. 2001-1062 of 15 November 2001 article 30 Official Journal of 16 November 2001) (modified by Law n°2014-1353 of 13 November 2014)

Without prejudice to any obligations relating to National Defence secrecy, officials to whom requests are made under the provisions of the present chapter are obliged to bring their support to justice.

3. Online search with the help of remote forensic software

Articles 706-102-1 to 706-102-9 PPC enable the judiciary to implement a technical device that aims to access computer data, in all places and without the consent of the concerned people, and to register, store, and transmit those data, as they are stored in the computer system, or as they are displayed on the screen of the user of the computer system, or as they are typed by the user of the system, or as they are transmitted or received and sent by audio-visual devices.

This procedure has already been studied previously in the current report since it enables to intercept correspondence in several respects.[440]

[440] In relation to conditions for implementation, see above the other sections of the current report relating to corresondence interception. Arts. 706-102-1 to 706-102-9 are in addition available in the Appendix.

IV. Use of Electronic Communication Data in Judicial Proceedings

France applies the rule of evidence by all means, subject to lawfulness and fairness, as long as this evidence can be discussed among the parties following the principle that both sides must be heard, in such a way that the right to a fair hearing is upheld.

A. Use of Electronic Communication Data in the Law of Criminal Procedure

Unless the law provides otherwise, evidence can be established by any means and the judge decides based on his or her personal conviction. This principle is established in relation to the judgement of misdemeanours[441] and also lies in the Civil Code.[442] In relation to the judgement of felonies, the Penal Procedure Code also establishes the principle that may be sought and taken into account any information that is likely to be useful to ascertain the truth.[443]

As a result, electronic communication data are admissible in justice in the same way as other proof, to the extent that their collection and the way they are presented before the court comply with legal requirements established in order to protect the rights of the accused[444] and fundamental rights more globally.[445]

This being said, the legal admissibility of evidence does not prejudge its probative value, which is partly regulated in the Penal Procedure Code[446] and the Civil Code in relation to electronic writing.[447]

- *Inter alia*, according to the Civil Code,[448] a writing consists of letters, characters, figures or of any other sign or symbol endowed with an intelligible meaning,

---

441 Art. 427 PPC.

442 Art. 1358 CC.

443 See, e.g., art. 81 related to judicial information and art. 310 (related to the production of evidence before the Court of Assize) PPC.

444 See below, Sections IV.B. and C.

445 See below, Section IV.B. and above, the conditions for collecting or intercepting communications, established in order to guarantee fundamental rights and primarily the secrecy of private life.

446 See notably art. 427 PPC. Production of evidence is regulated in arts. 427 to 457 PPC (in relation to misdemeanours) and in arts. 306 *et seq.* and 323 to 346 PPC (in relation to crimes).

447 Arts. 1358 *et seq.* CC.

448 The following translation of the CC articles is partly inspired from the translation proposed by Pierre Catala in *Proposals for Reform of the Law of Obligations and the Law of Prescription*, English translation by John Cartwright and Simon Whittaker, 2007, pp. 152 *et seq*. (arts. 1283 *et seq*. – the numbering of these articles has been changed in the

whatever its supports.[449] Electronic writing has the same probative value as a paper-based writing, provided that the person from whom it originates can be duly identified and that it is established and stored in a manner capable of assuring its integrity.[450] The signature which is necessary to complete a legal act identifies the person who places it on the document. It demonstrates his or her consent to the obligations which arise from the act. Where it is placed on the act by a public official, it confers authenticity on it. Where it is in electronic form, it consists of the use of a reliable process of identification, guaranteeing its link with the legal act to which it is attached. The reliability of the process is presumed, in the absence of proof of the contrary, where the electronic signature is created, the identity of the signatory is ensured, and the integrity of the legal act is guaranteed, under the conditions laid down by decree in Council of State.[451] Where the law has not laid down other principles, the judge settles conflicts between written evidence by determining using any means which is the more convincing instrument.[452]

- According to the Penal Procedure Code, a police record has probative value only if its form complies with legal requirements and if its author acted in the performance of their duties, on an issue falling within the scope of his of her responsibilities, and if he or she has reported what he or she has seen, heard, or noticed personally.[453]

B. Inadmissibility of Evidence as a Consequence of Inappropriate Collection

Evidence that is collected in violation of the requirements established in the Penal Procedure Code cannot be used in the proceedings where the latter Code provides explicitly for such penalty or where it provides for the nullity of the procedure of data collection or interception.[454] Where the Code is not clear on this issue, the inadmissibility of evidence may be decided by the judge upon request of the interested party.[455]

CC by a law of 2016), available at http://www.justice.gouv.fr/art_pix/rapportcatatla0905-anglais.pdf

[449] Art. 1365 CC.

[450] Art. 1366 CC.

[451] Art. 1367 CC.

[452] Art. 1368 CC.

[453] Art. 429 PPC.

[454] See the previous sections of this report in relation to interception orders requirements.

[455] See below, Section IV.C.

In addition, the Court of Cassation established a requirement of fairness of evidence, as a condition for the exercise of the rights of the defence, and, more generally, as condition for a fair trial.[456]

However, this requirement is more strictly enforced in relation to evidence produced by the public authority (or by a private party on the instructions of the public authority), in comparison with evidence produced by a private party.

1. Evidence produced by public authorities

Evidence produced by public authorities may be the result of certain positive acts, but it must not be the result of acts that caused the author to commit a penal infringement, in other worlds these acts must not have provoked or incited the commission of the penal infringement that is being proven.[457] More widely, the Court of Cassation rejects evidence obtained by fraudulent means.[458] Evidence thus obtained will be declared inadmissible,[459] and may even result in the nullity of proceedings.[460] However, the Court of Cassation does accept provocations that are not at the origin of the penal infringement, but which enable the infringement to be proven.[461]

In addition, it is to be noted that the Penal Procedure Code authorises judicial police officers and agents to commit certain penal infringements, for the purpose of the repression of certain misdemeanours and felonies. *Inter alia*, in relation to organised crime and attacks on automated data processing systems, these officers and agents may participate to electronic discussions with persons who are likely to have

---

[456] Pascal Lemoine, "La loyauté de la preuve (à travers quelques arrêts récents de la chambre criminelle)," Cour de cassation annual report 2004, available at https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2004_173/deuxieme_partie_tudes_documents_176/tudes_diverses_179/travers_quelques_6401.html#n_20_

[457] Cass. crim., 27 Feb. 1996, "Schuller" court case, bull. crim. 1996, n° 93; JCP 96, ed. G, II-22629, note M.-L. Rassat; D. 96, p. 346, note Ch. Guéry; Cass. crim., 11 May 2006, pourvoi n°05-84.837, bull. crim. 2006, n°132; see Pascal Lemoine, *op. cit*. See also Cour de cassation, rapport annuel 2012, *La preuve*, Livre 3, partie 4, Titre 2, Chapitre 2 – Admissibilité des modes de preuve, available at https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2012_4571/livre_3_etude_preuve_4578/partie_4_administration_preuve_4589/principes_gouvernant_4591/admissibilite_modes_26241.html

[458] Cass. crim., 28 Oct. 1991, bull. crim., n° 381; JCP, 1991.II.21704, note J. Pannier.

[459] Cass. crim., 9 Aug. 2006, n° 06-83.219, bull. crim. 2006, n° 202; Cass. crim., 7 Feb. 2007, pourvoi n° 06-87.753, bull. crim. 2007, n° 37; Cass. crim., 4 June 2008, pourvoi n° 08-81.045, bull. crim. 2008, n° 141; see Cour de cassation, rapport annuel 2012, *La preuve*, *op. cit*.

[460] Cass. crim., 27 Feb. 1996, bull. crim. 1996, n° 93.

[461] Cass. crim., 30 April 1998, pourvoi n° 97-85.747, bull. crim. 1998, n° 147; Cass. crim., 8 June 2005, pourvoi n° 05-82.012, bull. crim. 2005, n° 173; Cass. crim., 16 Jan. 2008, pourvoi n° 07-87.633, bull. crim. 2008, n° 14; see Cour de cassation, rapport annuel 2012, *La preuve, op. cit*.

committed an infringement and may gather evidence of this infringement within this framework.[462]

2. Evidence produced by private parties

The criminal chamber of the Court of Cassation considers that the judge does not have the power, based on articles 427 *et seq.* PPC, to reject evidence obtained by a party for the sole reason that this evidence has been unlawfully obtained.[463] Therefore, illegal and unfair means of proof may be accepted by French courts, where the evidence is provided by a private party, especially where the way the evidence has been collected was justified by the necessity of proving a fact and the impossibility of proving it otherwise.[464]

The judge must in such a case appreciate the probative value of the evidence.[465]

However, lawfulness and fairness are required where the private party who produces the evidence has acted in collaboration with public authority agents (under their instructions or with their assistance).[466]

C. The Right for the Accused to Challenge the Probity of Intercepted Data

A prerequisite for admissibility of evidence is that the produced evidence is submitted to a debate between the parties. This principle is established in the Penal Procedure Code[467] and is recalled by the Court of Cassation, particularly where it

---

462 Art. 706-87-1 PPC.

463 Cass. crim. 15 June 1993: bull. crim., n° 210 6 April 1993, JCP 1993, II, 22144, note M.-L. Rassat; see Pascal Lemoine, "La loyauté de la preuve (à travers quelques arrêts récents de la chambre criminelle)," *op. cit*.

464 Cass. crim., 31 Jan. 2007, pourvoi n° 06-82.383, bull. crim. 2007, n° 27. See Cour de cassation, rapport annuel 2012, *La preuve, op. cit*.

465 Cass crim., 15 June 1993, pourvoi n° 92-82.509, bull. crim. 1993, n° 210; Cass. crim., 6 April 1994, pourvoi n° 93-82.717, bull. crim. 1994, n°136; see Cour de cassation, rapport annuel 2012, *La preuve, op. cit*.

466 Ex. Cass. crim., 11 May 2006, pourvoi n° 05-84.837, bull. crim. 2006, n°132. See Cour de cassation, rapport annuel 2012, *La preuve, op. cit*.

467 Art. 427 PPC related to the production of evidences before the penal court judging misdemeanours, according to which evidence must be presented to the judge during court proceedings and be contradictorily discussed before him or her. Other parts of the PPC regulate specifically the production of evidence before the different courts: see especially arts. 278 *et seq*. in relation to the Court of Assize, which provide *inter alia* for the possibility, for the advocate, to access to all documents relevant to the proceedings (art. 278), and which clarifies that the judge must concisely elaborate evidence of charge and discharge during the course of the hearing (art. 327).

does accept the admissibility of some proofs obtained by illicit or unfair means, in order to ensure that such proofs do not entail a breach of the rights of defence.[468]

This implies that each of the parties can access the evidence produced by the other parties and has the time and the right to challenge this evidence.[469] As a result, the accused is empowered to challenge the means used and the procedure that has been followed in order to intercept electronic communications.

Proof to the contrary can in principle be established by any means, unless the law states otherwise, which is the case in very few matters. For example, where police records have been established by police officers or agents who received from a special legal provision the power of recording misdemeanours through police records, evidence to the contrary can only be produced in writing or by testimony.[470] Moreover, some special laws set out that some particular official records are considered to be valid proof until specific proceedings are launched to challenge the authenticity of facts.[471] Finally, written proof cannot result from correspondence between the accused and their attorney-at-law,[472] and the court can always order a forensic examination, if deemed necessary,[473] as well as complementary investigations.[474]

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

International judicial cooperation is regulated by articles 694 *et seq.* PPC. These provisions apply in the absence of any international convention or bilateral treaty stipulating otherwise.[475] Within the limits of the provisions of these articles, and within the limits of the powers for accessing electronic communications set out in the Penal Procedure Code, including article 100-8 which regulates some transborder situations,[476] mutual legal assistance may enable real-time access to electronic communication data.

---

468 See Court of Cassation, rapport annuel 2012, *La preuve*, *op. cit*.

469 This is especially organised in arts. 400 *et seq*., 427 *et seq*. and 458 *et seq*. PPC in relation to the judgment of misdemeanours and in arts. 283 *et seq*., 306 *et seq*. and 323 *et seq*. PPC in relation to the judgment of felonies.

470 Art. 431 PPC.

471 Art. 432 PPC.

472 Art. 433 PPC.

473 Arts. 434, 310 PPC.

474 Arts. 283, 436, and 456 PPC.

475 Art. 694 PPC.

476 See Appendix, Section A.

A first chapter dedicated to general provisions regulates the transfer and execution of judicial assistance requests (articles 694 to 694-4-1), assistance for the purpose of hearing, surveillance and infiltration (articles 694-5 to 694-9), and judicial assistance for the purpose of seizure of the proceeds of penal infringements with a view to subsequent confiscation (articles 694-10 to 694-13).

A second chapter dedicated to the provisions that are specific to judicial assistance between France and the other EU Member States regulates European Investigation Order (articles 694-15 to 694-50), joint investigation teams (articles 695-2 to 695-3), the Eurojust unit (articles 695-4 to 695-7), the Eurojust national representative (articles 695-8 and 695-9), the issue and execution of orders freezing property or evidence (articles 695-9-1 to 695-9-30), simplified exchange of information between services in application of the framework decision of the EU Council of 18 December 2006 (articles 695-9-31 to 695-9-49), cooperation between Asset Recovery Offices of Member States in the area of tracing and identifying proceeds of crimes and other goods in relation to crime, in application of Decision 2008/845/JHA of the Council of 6 December 20017 (articles 695-9-50 to 695-9-53), and the prevention and resolution of conflicts of competence exercise in application of the framework decision of the Council of the European Union of 30 November 2009 (articles 695-9-54 to 695-9-57).

A third chapter contains one provision pertaining to judicial assistance between France and certain States (article 695-10).

A fourth chapter contains provisions regulating the European arrest warrant, procedures for transfer between Member States resulting from the EU Council framework decision of 13 June 2002 and procedures for transfer resulting from agreements concluded by the European Union and other States (articles 695-11 to 695-58).

In addition, France has ratified the Council of Europe Convention on cybercrime with two reservations in relation to the procedure. Firstly, "France reserves itself the right not to establish jurisdiction when the offence is committed outside the territorial jurisdiction of any State."[477] Secondly, France declared that "whenever the offence is punishable under criminal law where it has been committed, proceedings shall be instituted only upon request from the district prosecutor and must be preceded by a complaint from the victim or his/her beneficiaries or by an official complaint from the authorities of the State where the act was committed."[478]

---

[477] Council of Europe, Reservations and Declarations for Treaty No.185 – Convention on Cybercrime, France, status as of 18/02/2019, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=DVkVUK3n&_coeconventions_WAR_coeconventionsportlet_enVigueur=false&_coeconventions_WAR_coeconventionsportlet_searchBy=state&_coeconventions_WAR_coeconventionsportlet_codePays=FRA&_coeconventions_WAR_coeconventionsportlet_codeNature=2

[478] *Ibid.*

B. Requirements and Procedure

1. General provisions regulating requests for judicial assistance

Beyond article 100-8 PPC which regulates requests for interception addressed by the French judge to competent authorities,[479] requests for judicial assistance are regulated by articles 694 *et seq.* of the same Code[480] where they do not take place within the framework of a European Investigation Order.

Requests for judicial assistance from the judicial authorities of another State and addressed to French judicial authorities are transmitted through diplomatic channels. In urgent cases they may be directly sent to the district prosecutor or the investigating judge of the territorially competent district court (depending on the authority that is competent to enforce them), possibly through the general prosecutor, but they must be the subject of an opinion sent through diplomatic channels by the foreign government concerned unless there is an international convention stipulating otherwise.[481]

Requests for judicial assistance must be executed in accordance with the procedural rules provided by the Penal Procedure Code, including guarantees protecting persons subject to the measure.[482] However, they may be executed in accordance with the procedural rules indicated by the competent authorities of the requesting State, in case the request specifies it, under the reserve (under penalty of nullity) that these rules do not reduce the rights of the parties or the procedural guarantees provided for by the Penal Procedure Code.[483]

2. Provisions specific to cooperation between France and other EU Member States

Most of these provisions have been included in the Penal Procedure Code by an Ordinance n° 2016-1636 of December 2016,[484] which created articles 694-14 to 694-50 (beside article 100-8[485]), aiming especially at implementing the provisions of Directive 2014/41/EU regarding the European Investigation Order. These new provisions are enforceable since 22 May 2017.[486]

---

479 See Appendix, Section A.

480 See above, Section V.A.1.

481 Arts. 694 to 694-2 PPC. See Appendix, Section E.

482 Arts. 694-3 PPC. See Appendix, Section E.

483 Arts. 694-3 PPC. See Appendix, Section E.

484 Ordinance n° 2016-1636 of 1 December 2016, JORF n° 0280 of 2 December 2016, text n° 37.

485 See Appendix, Section A.

486 Art. 5 of Ordinance n°2016-1636.

Beside these provisions, articles 695-2 and 695-3 regulate especially joint investigation teams.

a) European Investigation Orders

Unless the Penal Procedure Code states otherwise, request for legal assistance between France and other EU Member States are executed through European Investigation Orders.[487] Any European Investigation Orders transmitted to French authorities must be issued or validated by a judicial authority.[488] It is addressed to the district prosecutor or to the investigating judge who is competent.[489] The magistrate who is seized may refuse to recognise or to execute the order in several situations described in article 694-31 PPC, including non-exhaustively the case where the order is contrary to the establishment of penal liability in the area of press infringements, and the case where exist serious reasons to believe that the execution of the order would be incompatible with the respect, by the French State, of the rights and freedoms guaranteed by the European Convention on Human Rights and the European Union Charter for Fundamental Rights.

The European Investigation Order is executed in compliance with forms and procedures set out by the requesting authority, under the reserve (under penalty of nullity) that these rules do not reduce the rights of parties and of procedural guarantees that enforce the fundamental principles established in the preliminary article of the Penal Procedure Code.[490, 491]

b) Joint investigations teams

A joint investigation team may be created where there is need to carry out, in the context of a French prosecution, either complex inquiries involving the mobilisation of extensive resources and which concern other Member States or where several Member States are carrying out inquiries into offences which call for coordinated and concerted action between the Member States concerned, with the prior agreement of the Minister of Justice and the consent of the Member State or States concerned.[492]

---

487 Art. 694-15 PPC.

488 Art. 694-29 PPC.

489 Art. 694-30 PPC.

490 These principles are *inter alia* those of a fair trial, of the presumption of innocence and of appeal.

491 Art. 694-36 PPC.

492 Art. 695-2 PPC. This paragraph quotes the English translation of the latter article proposed in the PPC translated by Legifrance at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf. See Appendix, Section A.

In the context of a joint investigation team, French judicial police officers and agents attached to a joint investigation team may carry out operations ordered by the head of the team, over the whole of the territory of the State in which they are operating, within the limit of the powers conferred on them by the Penal Procedure Code. Their tasks are defined by the authorities of the Member State competent to direct the joint investigation team in the territory where the team is working. They may receive statements and record offences in the forms provided for by the Penal Procedure Code, subject to the consent of the State in whose territory they are operating.[493]

c) Simplified exchange of information, implementing Decision 2006/960/JAI of 18 December 2006

The simplified exchange of information, implementing Decision 2006/960/JAI of 18 December 2006, is regulated in articles 695-9-31 to 695-9-49.

Article 695-9-31 authorises National police and gendarmerie services and certain custom, finance and Ministry of the Interior's services to exchange, with competent services of another Member State, information that is at their disposal, in the aim of preventing a penal infringement, of collecting evidence in relation with a penal infringement or of searching for perpetrators of a penal infringement, either they detain it or they can access it, especially through the consultation of a data processing system, without making it necessary to take or ask for a requisition measure or another coercive measure.

Article 695-9-32 sets out that exchanged information is confidential, which must be guaranteed by its means of transmission and of storage.

The following provisions regulate requests for information issued by French services (articles 695-9-33 to 695-9-36) and requests for information received by French services (articles 695-9-37 to 695-9-47).[494] Upon request of competent foreign services, the French services and units mentioned in article 695-9-31 transmit the requested information, providing that it complies with this same article 695-9-31 and that it is useful in order to prevent a penal infringement, or that is useful to conduct investigations aiming at establishing evidence of a penal infringement or at searching for its perpetrators.[495]

---

[493] Art. 695-3 PPC. This paragraph quotes the English translation of the latter article proposed in the PPC translated by Legifrance at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf. See Appendix, Section E.

[494] See Appendix, Section E. Following information is largely issued from the English translation proposed in the PPC translated by Legifrance at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf

[495] Art. 695-9-37 PPC.

If the information mentioned in article 695-9-31 may be useful to another Member State to prevent one of the penal infringements mentioned in article 695-32[496] and punished by at least three years of imprisonment, or if this information may be useful to this other Member State in order to conduct investigations aiming at establishing evidence of such a penal infringement or to search for its perpetrators, the service or unit that holds this information transmits it to this other Member State without the need to have received a corresponding request.[497]

When this information is initially transmitted by another Member State on the basis of the framework decision 2006/960/JAI, it may only be transmitted to another Member State following the conditions imposed by the first transmitting Member State. When this information is initially transmitted by another Member State on a basis other than the framework decision 2006/960/JAI, or by a non-EU Member State, it may only be transmitted to another Member State with the agreement of the first transmitting State and under the conditions imposed by this State, in all the situations where France must respect these principles according to an international agreement.[498]

Information can only be transmitted to the relevant services of the Member State that requested it, with the authorisation of a judge, each time such an authorisation is mandatory under French law in order to access this same information or to transmit this same information to a judicial police service or unit. The request for authorisation is addressed to the relevant judge by the service or unit to which the information is requested. Elements of an ongoing penal procedure can only be transmitted with the authorisation of the investigating court in charge of the case, or with the authorisation of the district prosecutor when the trial court has been seized.[499]

Services or units mentioned in article 695-9-31 cannot refuse to communicate information requested by a Member State, unless reasons exist to think that such communication:

– could be prejudicial to the fundamental interests of the State in terms of national security;
– could be prejudicial to ongoing investigations in penal matters or would jeopardise people's security;
– or would be clearly disproportionate or pointless in relation to the purposes for which the information has been requested (article 695-9-41).

---

[496] Art. 695-32 PPC lists several penal infringements including (non-exhaustively) participation in a criminal organisation, terrorism, human trafficking, child pornography and sexual exploitation of children, cybercrime.

[497] Art. 695-9-38 PPC, modified by Ordinance n° 2016-1636.

[498] Art. 695-9-39 PPC.

[499] Art. 695-9-40 PPC.

In addition, the Penal Procedure Code provides for other possibilities to refuse requested information.[500]

On the occasion of the transmission of the information, the service or unit mentioned in article 695-9-31 indicates to the receiving service the conditions of use of the information. Each time it deems it is necessary, it may ask the receiving service to provide information about the use that has been made of the transmitted information.[501]

Where information has been transmitted by a service or unit mentioned in article 695-9-31 to the relevant service of a Member State and where the latter considers transmitting it to another State or using it for a purpose other than the one for which the transmission was permitted, the service or unit that made the original transmission is competent to consider whether the new transmission or the new use should be authorised, on the request of the receiving State, and, if needed, to determine the conditions of it.[502]

Information transmitted by the service or unit mentioned in article 695-9-31 may be used by the receiving service as evidence, unless it was otherwise stipulated on the occasion of its transmission.[503]

Information transmitted by the service or unit mentioned in article 695-9-31 to the relevant service of a Member State is also transmitted to the Eurojust and Europol units, to the extent it relates to a penal infringement falling within their mandate.[504]

Contact points to whose requests for transmission of information can be addressed by relevant services of Member States are nominated by order of the Ministry of Justice, of the Ministry of the Interior and of the Ministry responsible for the budget.[505]

3. Other provisions

Provisions regulating simplified exchange of information are applicable to States that are not members of the European Union but which are associated with the implementation, the application, and the development of the Schengen *acquis*, according to article 695-9-48 PPC. Conditions of implementation are determined by a decree issued by the Council of State (article 695-9-49).

---

500 See art. 695-9-42 PPC in the Appendix, Section E.

501 Art. 695-9-43 PPC.

502 Art. 695-9-44 PPC.

503 Art. 695-9-45 PPC.

504 Art. 695-9-46 PPC.

505 Art. 695-9-47 PPC.

Appendix

A. Interception of the Content of Electronic Communications under Articles 100 *et seq.* of the Penal Procedure Code

Article 100

For the investigation of felonies and misdemeanours, if the penalty incurred is equal to or in excess of two years' imprisonment, the investigating judge may order the interception, recording and transcription of correspondence transmitted by means of electronic communication where the requirements of the investigation call for it. Such operations are made under his authority and supervision.

The interception decision is made in writing. It is not a jurisdictional decision and cannot be appealed.

Article 100-1

The order made pursuant to article 100 must include all the details identifying the link to be intercepted, the offence which justifies resorting to an interception, and the duration of this interception.

Article 100-2

This decision can last for a maximum duration of four months. It may be extended only by following the same conditions as to form and duration, without the total period of interception being longer than one year, or, if is concerned an infringement under articles 706-73 and 706-73-1, two years.

Article 100-3

The investigating judge or the judicial police officer appointed by him may require any qualified agent of a service or body placed under the authority or supervision of the Minister in charge of electronic communication, or any qualified agent of an authorised network operator or purveyor of electronic communication services to set up an interception device.

Article 100-4

The investigating judge or the judicial police officer appointed by him drafts an official record of both the interception and recording operations. This official record mentions the date and time when the operation started and ended.

The recordings are placed under closed official seals.

Article 100-5

The investigating judge or the judicial police officer appointed by him transcribes any correspondence which is useful for the discovery of the truth. An official record is made of these transcriptions. The transcription is attached to the case file.

Correspondence in a foreign language is transcribed into French with the assistance of an interpreter appointed for this purpose.

On penalty of nullity, no transcription may be made of any correspondence with an advocate relating to the exercise of the defendant's rights.

On penalty of nullity, no transcription may be made of any correspondence with a journalist allowing identifying a source in breach of Article 2 of the Law of 29 July 1881 on Freedom of the Press.

Article 100-6

The recordings are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution.

An official record is made of the destruction.

Article 100-7

No interception may be made on the telephone line of a member of Parliament or senator unless the president of the assembly he belongs to is informed of the interception by the investigating judge.

No interception may be made on a telephone line connecting the chambers or domicile of an advocate unless the president of the bar association is informed of this by the investigating judge.

No interception may be made on a telephone line connecting the chambers or domicile of a judge or prosecutor unless the president or the prosecutor general of the court with jurisdiction over the area in question is informed of this by the investigating judge.

The formalities set out by the present article are prescribed under penalty of nullity.

Article 100-8

Where an interception of correspondence transmitted by means of electronic communication targets an address of communication which is used on the territory of a Member State of the European Union, whereas it does not take place within the framework of a European investigation order, the investigating judge or the judicial police officer appointed by him notifies this interception to the competent authority of this State where the person concerned is located on its territory.

This notification shall take place either before the interception where it appears from the elements contained in the record of the proceedings at the time the interception is ordered, that the targeted person is or will be on the territory of this State, or during the course of the interception or after it has been made, as soon as it is established that the targeted person is or was on this territory at the time of interception.

Upon request by the competent authority of the Member State, made within ninety six hours from receipt of the notification and justified by the fact that such interception could not be authorised, within the framework of a similar national proceeding, under the law of that State, either the interception cannot be carried out or it must be interrupted, or intercepted data while the person was on its territory cannot be used and must be removed from the record of the proceedings or can be used only under the conditions specified by this authority and for the reasons it specifies.

The absence of the act of notification provided for in the first and second paragraphs is considered to be a cause for nullity of proceedings only where it is established that such interception could not be authorised within the framework of a similar national proceeding, under the law of the Member State on whose territory was the targeted person.

Article 80-4

During the course of an inquiry into the death or disappearance of a person set out in articles 74 and 74-1, the investigating judge proceeds pursuant to the provisions of Chapter 1 of Title 3 of Book 1. The interception of telecommunication correspondence is carried out under his authority and control under the conditions laid down in the second paragraph of article 100 and in articles 100-1 to 100-7. This interception may not exceed a period of two months, which is renewable.

The family members or close relations of the deceased or missing person may exercise civil party rights as accessories. However, where the missing person is found, the latter's address and other matters that would lead to the direct or indirect disclosure of this address may not be revealed to the civil party without the consent of the party concerned, if he is an adult, or with the consent of the investigating judge in the case of minors or of adults under guardianship orders.[506]

Article 709-1-3

If there are reasonable grounds to believe that, at the end of his or her incarceration, a sentenced person did not respect its obligation, pursuant to the sentence, to not contact certain persons or certain categories of persons, to not socialise with other sentenced persons or to not frequent one given place, a category of places or a specially identified zone, police services and Gendarmerie units may, on instruction of the judge responsible for the enforcement of sentences or, under article 131-9, §2 or under article 131-11, §2 of the penal Code, on instruction of the judge responsible for the enforcement of sentences required for this purpose by the district prosecutor, perform, throughout the national territory, if these measures are indispensable in order to prove the violation of prohibitions resulting from the sentence:

1° In relation to a felony or a misdemeanour mentioned in article 100 §1 of the current Code, the intercept, the recording and the transcript of correspondence transmitted by means of telecommunications, in accordance with the procedures laid down in subsection 2 of section 3 of Chapter I of Title III of Book I *(Ed: referring to article 100 to 100-8).*

2° In relation to a felony or a misdemeanour mentioned in §1 and 2 of article 230-32[507], to the real-time localisation of a person, without his or her knowledge, of a vehicle or of any other object, without the consent of his or her owner or possessor, in accordance with the procedures laid down in Chapter V of Title IV of Book I *(Ed: referring to article 230-32 to 230-44 which regulate geolocation).*

B. Interceptions of Communications for the Purpose of Organised Crime and Delinquency Repression

1. Provisions authorising communications interception

a) Interception of correspondence in preliminary and flagrancy investigations

Article 706-95:

If the needs of a flagrancy inquiry or a preliminary inquiry into one of the offences within the scope of articles 706-73 and 706-73-1[508] justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor, authorise the interception, recording or transcription of correspondence by electronic communication, under the provisions of paragraph two of article 100, article 100-1 and articles 100-3 to 100-7, for a maximum period of one month, renewable once under the same conditions of form

---

[506] This translation is proposed by the Centre for civil and political rights, with the participation of John Rason SPENCER QC, and is available at http://ccprcentre.org/doc/HRC/Tunisia/Alkarama_Tunisia_FU_fr.pdf

[507] See below, Section C.

[508] See below, Section B.2.

and duration. These operations are carried out under the supervision of the liberty and custody judge.

The provisions of Article 100-8 are applicable to interceptions ordered under the current Article.

For the application of the provisions of articles 100-3 to 100-8, the powers conferred on the investigating judge or the judicial police officer nominated by him are exercised by the district prosecutor or the judicial police officer appointed by him.

The liberty and custody judge who has authorised this interception is informed without undue delay by the district prosecutor of any actions carried out in accordance with the previous paragraph, including official records drawn-up pursuant to his authorisation, by way of the application of articles 100-4 and 100-5.

b) Interception of technical connection data, geolocation data, and correspondence sent or received by terminal equipment

The interception of technical connection and geolocation data, as well as electronic correspondence sent or received by terminal equipment is set out in articles 706-95-4 to 706-95-10 PPC.[509]

Article 706-95-4

I.-If the needs of an inquiry into one of the offences within the scope of articles 706-73 and 706-73-1 of the current Code justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor, authorise judicial police officers to use a technical device or apparatus mentioned in 1° of article 226-3 of the Penal Code[510]

---

[509] An English translation of these articles taking into account modifications of the law up to 2005 is found at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf (art. 706-95 was modified by a law of 2015 and afterward by an ordinance of December 2016; articles 706-95-4 to 706-95-10 have been created by law n° 2016-731 of 3 June 2016).

[510] Art. 226-3 PC punishes by a prison term of 5 years and a fine of €300,000: (1) The manufacture, import, detention, exhibition, offer, rental or sale of apparatuses or of technical devices whose nature is such that they may enable to perform operations that constitute the offence set out under the second paragraph of art. 226-15 PC or which, being designed for the detection of conversations from a distance, enable the commission of an offence under art. 226-1 PC, or which purpose is to capture computer data under articles 706-102-1 and 706-102-2 PPC and L. 853-2 ISC and which are enumerated on a list drawn up pursuant to the conditions determined by decree of the Conseil d'Etat, where such acts are committed, including by negligence, in the absence of a ministerial authorisation whose conditions of granting are determined by that decree or if they are committed without respecting the conditions provided for in this authorisation; (2) The advertising of an apparatus or a technical device liable to enable the commission of the offences set out under article 226-1 and the second paragraph of article 226-15, where this advertisement constitutes an incentive to commit such offences or the advertising of an apparatus or a technical device whose purpose is computer data capture under articles 706-102-1 and 706-102-2 PPC and L. 853-2 ISC where this advertisement constitutes an incentive to use it fraudulently.

Art. 226-1 punishes by a penalty of one year's imprisonment and a fine of €45,000 any wilful violation of the intimacy of the private life of other persons by resorting to any means of: 1° intercepting, recording or transmitting words uttered in confidential or private circumstances, without the consent of their speaker; 2° taking, recording or transmitting

in order to collect technical connection data that enable to identify a terminal equipment or its user's subscription number, as well as data related to the location of the terminal equipment used. The authorisation is delivered for a maximum period of one month, renewable once under the same conditions.

II.-The liberty and custody judge of the district court may also, under the same conditions, authorise the use of this device or apparatus in order to intercept correspondence sent or received by a terminal equipment. In this situation the procedures laid down in articles 100-4 to 100-7 of the current Code are applicable and the powers conferred to the investigating judge or to the judicial police officer appointed by him are exercised by the district prosecutor or to the judicial police officer appointed by this magistrate. The authorisation is delivered for a maximum period of forty-eight hours, renewable once under the same conditions.

III.-In case of emergency resulting from an imminent risk of evidence being damaged or an imminent risk of serious harm to persons or goods, the authorisation mentioned in the I and II may be delivered by the district prosecutor. It includes a statement on the factual circumstances that establish the existence of the imminent risk. The authorisation must then be confirmed by the liberty and custody judge within a maximal period of twenty four hours. Failing that, the operation is brought to an end, collected data or correspondence are placed under closed official seals and cannot be exploited or used in the proceedings.

The liberty and custody judge who delivered or confirmed the authorisation is informed without undue delay by the district prosecutor with regard to acts that have been performed under the current article and with regard to official records drawn-up pursuant to his authorisation.

Article 706-95-5

I.-If the needs of a judicial investigation into one of the offences within the scope of articles 706-73 and 706-73-1 of the current Code justify this, the investigating judge may, after obtaining the opinion of the district prosecutor, authorise judicial police officers to use a technical device or apparatus mentioned in 1° of article 226-3 of the Penal Code in order to collect technical connection data that enable to identify a terminal equipment or its user's subscription number, as well as data related to the location of the terminal equipment used. The authorisation is delivered for a maximum period of two months, renewable under the same conditions, without the total period of operations being longer than six months.

II.-The investigating judge may also, under the same conditions, authorise the use of this device or apparatus in order to intercept correspondence sent or received by a terminal equipment. In this situation the procedures laid down in articles 100-4 to 100-7 of the current Code are applicable. The authorisation is delivered for a maximum period of forty-eight hours, renewable once under the same conditions.

---

the picture of a person who is within a private place, without the consent of the person concerned. Where the offences referred to in the present article were performed in the sight and with the knowledge of the persons concerned without their objection, although they were in a position to do so, their consent is presumed;

Art. 226-15, §2 punishes by a prison term of 1 year and a fine of €45,000 the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by electronic means, or the setting up of a device whose nature is such that it might enable to achieve such interceptions.

Article 706-95-6

Authorisations mentioned in articles 706-95-4 and 706-95-5 shall be the subject of a written order stating the reasons for the authorisation. This order does not constitute a jurisdictional decision and cannot be appealed.

Article 706-95-7

Operations mentioned in articles 706-95-4 and 706-95-5 are carried out under the authority and supervision of the magistrate who authorised them and cannot, under penalty of nullity, pursue another purpose than that of investigating and detecting penal infringements that are mentioned in the decision of this magistrate.

The fact that these operations reveal penal infringements other than those mentioned in the magistrate's decision that authorises these operations is not a cause for nullity of incidental proceedings.

Article 706-95-8

The district prosecutor, the investigating judge or the judicial police officer may require any qualified agent of a service, of a unit or of a body placed under the authority of the Ministry of the Interior, the list of which is set by decree, with a view to proceeding with the use of the technical device or apparat mentioned in articles 706-95-4 and 706-95-5.

Article 706-95-9

The judicial police officer draws-up an official record of operations carried out under the I of articles 706-95-4 and 706-95-5. This official record mentions the date and time at which each of the necessary operations started and at which these operations ended.

The judicial police officer attaches to the official record the collected data that are useful for ascertaining the truth

Article 706-95-10

Collected data pursuant to the I of articles 706-95-4 and 706-95-5 are destroyed, on the initiative of the district prosecutor or of the public prosecutor, at the date on which prosecution is barred under the statute of limitations or when a final decision has been given on the substance. An official record is made of the destruction.

Correspondences intercepted pursuant to II of articles 706-95-4 and 706-95-5 can only relate to the person or to the communication link referred to in the authorisation of interception operations.

c) Interception of stored correspondence

Since Law n°2016-731 of 3 June 2016, the interception of stored electronic correspondence is set out in articles 706-95-1 to 706-95-3 PPC:

Article 706-95-1

If the needs of an inquiry into one of the offences within the scope of articles 706-73 and 706-73-1 justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor, authorise, by way of reasoned order, access, remotely and without the knowledge of the person concerned, to correspondence stored by means of electronic communication and accessible using an electronic identifier. Data to which access has been enabled can be seized and registered or copied on any support.

Article 706-95-2

If the needs of a judicial information into one of the offences within the scope of articles 706-73 and 706-73-1 justify this, the investigating judge may authorise, by way of rea-

soned order, access, remotely and without the knowledge of the person concerned, to correspondence stored by means of electronic communication and accessible using an electronic identifier. Data to which access has been enabled can be seized and registered or copied on any support.

Article 706-95-3

Operations mentioned in articles 706-95-1 and 706-95-2 are carried out under the authority and the supervision of the magistrate who authorised them and cannot, under penalty of nullity, pursue another purpose than that of investigating and detecting penal infringements that are mentioned in the decision of this magistrate.

The magistrate or the judicial police officer appointed by him may require any qualified agent of a service or body placed under the authority or supervision of the Minister in charge of electronic communication, or any qualified agent of an authorised network operator or purveyor of electronic communication services to set up the operations mentioned in articles 706-95-1 and 706-95-2.

The fact that these operations reveal penal infringements other than those mentioned in the magistrate's decision that authorises these operations is not a cause for nullity of incidental proceedings.

Where the electronic identifier is linked to the account of an advocate, of a magistrate, of a member of the Parliament or of a senator, article 100-7 is applicable.

d) Remote data capture

Remote data capture is set out in articles 706-102-1 to 706-102-9 PPC:[511]

Article 706-102-1

If the needs of an inquiry into one of the penal infringements within the scope of articles 706-73 and 706-73-1 justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor, authorise, by way of reasoned order, judicial police officers and agents that have been appointed by the district prosecutor, to implement a technical device aiming to access computer data, in all places and without the consent of the concerned people, and to register, store and transmit those data, as they are stored in the computer system, or as they are displayed on the screen of the user of the computer system, or as they are typed by the user of the system, or as they are received and sent by audio-visual devices.

The district prosecutor may appoint any entitled natural or legal person who is registered in one of the lists provided for in article 157, in order to perform the technical operations that allow the realisation of the technical device mentioned in the first paragraph of the current article. The district prosecutor may also prescribe the use of the State's means that are covered by confidentiality for national defence purposes in accordance with the forms laid down by Chapter Ist of Title IV of Book Ist.

Article 706-102-2

If the needs of a judicial investigation into one of the penal infringements within the scope of articles 706-73 and 706-73-1 justify this, the investigating judge may, after having requested the opinion of the district prosecutor, authorise, by way of reasoned order, judicial police officers and agents that have been appointed by rogatory commission, to implement a technical device aiming to access computer data, in all places and without the consent of the concerned people, and to register, store and transmit those da-

---

[511] See note on English translation of these articles above. However, these articles have been modified by Law n°2016-731 of 3 June 2016.

ta, as they are stored in the computer system, or as they are displayed on the screen of the user of the computer system, or as they are typed by the user of the system, or as they are received and sent by audio-visual devices.

The investigating judge may appoint any entitled natural or legal person who is registered in one of the lists provided for in article 157, in order to perform the technical operations that allow the realisation of the technical device mentioned in the first paragraph of the current article. The investigating judge may also prescribe the use of the State's means that are covered by confidentiality for national defence purposes in accordance with the forms laid down by Chapter Ist of Title IV of Book Ist.

Article 706-102-3

Under penalty of nullity, the decision of the liberty and custody judge of the district court or of the investigating judge, taken pursuant to articles 706-102-1 and 706-102-2, mentions the penal infringement that justifies the operation, the exact location or the comprehensive description of the computer systems concerned and the duration of operations.

The authorisation decision taken pursuant to article 706-102-1 is delivered for a maximum duration of one month, renewable once under the same conditions. The authorisation decision taken pursuant to article 706-102-2 is delivered for a maximum duration of four months, renewable under the same conditions, without the total period of operations being longer than two years.

Article 706-102-4

The operations provided for in the current section are carried out under the authority and the supervision of the magistrate who authorised them, who may at all time order their interruption. Under penalty of nullity, these operations cannot pursue another purpose than that of investigating and detecting penal infringements that are mentioned in the decisions of this magistrate.

The fact that these operations reveal penal infringements other than those mentioned in these decisions is not a cause for nullity of incidental proceedings.

Article 706-102-5

In order to implement the technical device mentioned in articles 706-102-1 and 706-102-2, the liberty and custody judge of the district court, at the request of the district prosecutor, or the investigating judge, may authorise the introduction to a vehicle or to a private place, including outside the times mentioned in article 59 of the Penal Procedure Code,[512] without the knowledge or without the consent of the owner or of the possessor of the vehicle or of the occupier or of any person having a right to this vehicle or place. If the device must be introduced in a home outside the times mentioned in article 59, this authorisation must be delivered by the liberty and custody judge of the district court, on the special request of the district prosecutor or by the investigating judge. These operations cannot pursue any other aim than implementing the technical device and are performed under the authority and supervision of the liberty and custody judge or of the investigating judge. The current paragraph is also applicable to operations aimed at uninstalling the technical device that has been implemented.

In order to implement the device mentioned in articles 706-102-1 and 706-102-2, the liberty and custody judge of the district court, at the request of the district prosecutor or the investigating judge may also authorise the transmission of this device by means of an electronic communications network. These operations are performed under the au-

---

[512] Art. 59 states that, except where they are requested from within a building or in the exceptional cases provided for by law, searches and house visits may not be undertaken before 6 am or after 9 pm.

thority and supervision of the liberty and custody judge of the district court or of the investigating judge. The current paragraph is also applicable to operations aiming at uninstalling the technical device that has been implemented.

The technical device mentioned in article 706-102-1 can neither be implemented in a computer system located in places covered by articles 56-1,[513] 56-2[514], 56-3[515] and 56-5,[516] nor in the vehicle, the business premises or the home of people mentioned in article 100-7.

Article 706-102-6

The investigating judge or the judicial police officer appointed by him or required by the district prosecutor may require any qualified agent of a service or unit or body placed under the authority or supervision of the Ministry of the Interior or of the Ministry of Defence, a list of which is determined by means of a Decree, in order to install the device mentioned in articles 706-102-1 and 706-102-2.

Article 706-102-7

The investigating judge or the judicial police officer appointed by him or required by the district prosecutor draws-up an official record of both the operations of installation of the device mentioned in articles 706-102-1 and 706-102-2, and the operations of computer data capture. This official record mentions the date and times when the operation started and the date and time when the operation ended.

The recordings of computer data are placed under closed official seals.

Article 706-102-8

The investigating judge or the judicial police officer appointed by him or required by the district prosecutor describes or transcribes, in an official record filed in the criminal case file, the data that are useful to ascertain the truth. No sequence relating to private life but that has no relation with penal infringements mentioned in the decisions that authorise the measure can be kept in the criminal case file.

Data in a foreign language are transcribed into French with the assistance of an interpreter appointed for this purpose.

Article 706-102-9

The recordings of computer data are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution.

An official record is made of the destruction.

In addition, the Penal Procedure Code organises the remote capture of spoken words in a private place or under confidentiality and images in a private place (articles 706-96 to 706-102 of the Penal Procedure Code).

---

513 This article refers to business premises or the home of advocates.

514 This article refers to business premises of media companies, audio-visual communication companies, online public communication companies, press agencies, to the professional vehicles of these companies and to journalists' home where the investigation is relating to this journalist's professional activities.

515 This article refers to professional premises of doctors, notaries, or bailiffs.

516 This article refers to seizures taking place at judicial premises and at the home of people exercising judicial office, and aiming at seizing documents likely to be covered by deliberation secrecy.

e) Capture of private words or images

The capture of private words or images is set out in articles 706-96 to 706-PPC:

Article 706-96

If the needs of an investigation into one of the penal infringements within the scope of articles 706-73 and 706-73-1 justify this, the liberty and custody judge may, upon request of the district prosecutor, authorise judicial police officer and agents to implement a technical device having the object, without the consent of the person concerned, caption, fixation, transmission and recording of words spoken privately or confidentially by one or several persons that are located in a private place.

In order to implement the technical device mentioned in the first paragraph of the current article, the liberty and custody judge may authorise the intrusion in a vehicle or a private place, including outside times mentioned in Article 59, without the knowledge or without the consent of the owner or of the possessor of the vehicle or of the occupier or of any person having a right to this vehicle or place. These operations, which cannot pursue another aim than the one of implementing the technical device, are performed under his supervision. The current paragraph is also applicable to operations aiming to uninstall the implemented technical device.

The implementation of the technical device mentioned in the first paragraph cannot concern places mentioned in articles 56-1, 56-2, 56-3 and 56-5 and cannot take place in the vehicle, in the office or at the home of persons mentioned in article 100-7.

Article 706-96-1

If the needs of a judicial investigation into one of the penal infringements within the scope of articles 706-73 and 706-73-1 justify this, the investigating judge may, after having requested the opinion of the district prosecutor, authorise judicial police officer and agents to implement a technical device having the object, without the consent of the person concerned, caption, fixation, transmission and recording of words spoken privately or confidentially by one or several persons that are located in a private place.

In order to implement the technical device mentioned in the first paragraph of the current article, the investigating judge may authorise the intrusion in a vehicle or a private place, including outside times mentioned in Article 59, without the knowledge or without the consent of the owner or of the possessor of the vehicle or of the occupier or of any person having a right to this vehicle or place. If a home is concerned and if the operation must take place outside times mentioned in Article 59, this authorisation is delivered by the liberty and custody judge requested for this purpose by the investigating judge. These operations, which cannot pursue another aim than the one of implementing the technical device, are performed under the supervision of the investigating judge. The current paragraph is also applicable to operations aiming to uninstall the implemented technical device.

The implementation of the technical device mentioned in the first paragraph cannot concern places mentioned in articles 56-1, 56-2, 56-3 and 56-5 and cannot take place in the vehicle, in the office or at the home of persons mentioned in article 100-7.

Article 706-97

Authorisations mentioned in articles 706-96 and 706-96-1 are subject of a written and reasoned order which mentions all the details that enable to identify vehicles or private or public places concerned, the penal infringement that justifies the operation and the duration of operations. This order is not a jurisdictional decision and cannot be appealed.

Article 706-98

The authorisation decision taken pursuant to article 706-96 is delivered for a maximum duration of one month, renewable once under the same conditions.

The authorisation decision taken pursuant to article 706-96-1 is delivered for a maximum duration of two months, renewable under the same conditions, without the total period of operations being longer than two years.

Article 706-98-1

The operations provided for in articles 706-96 and 706-96-1 are carried out under the authority and the supervision of the magistrate who authorised them.

The fact that these operations reveal penal infringements other than those mentioned in these decisions is not a cause for nullity of incidental proceedings.

Article 706-99

The district prosecutor, the investigating judge or the judicial police officer appointed pursuant to articles 706-96 and 706-96-1 may require any qualified agent of a service or unit or body placed under the authority or supervision of the Ministry of the Interior or of the Ministry of Defence, a list of which is determined by means of a Decree, in order to install the technical devices mentioned in articles 706-96 and 706-96-1.

Article 706-100

The district prosecutor, the investigating judge or the judicial police officer appointed pursuant to articles 706-96 and 706-96-1 draws-up an official record of each of the operations of installation of the technical device and of the operations of capture, fixation, and sound or audio-visual recording. This official record mentions the date and times when the operation started and the date and time when the operation ended.

Recordings are placed under closed official seals.

Article 706-101

The district prosecutor, the investigating judge or the judicial police officer appointed pursuant to articles 706-96 and 706-96-1 describes or transcribes, in an official record attached to the case file, the recorded images and conversations that are useful to ascertain the truth. No sequence relating to private life but that has no relation with penal offences referred to in the decisions that authorise the measure can be kept in the case file.

Conversations in foreign language are transcribed into French with the assistance of an interpreter appointed for this purpose.

Article 706-101-1

The liberty and custody judge who authorised the operation mentioned in article 706-96 is informed without undue delay by the district prosecutor about acts that have been accomplished pursuant to this same article 706-96 and about official records that have been drawn-up pursuant to articles 706-100 and 706-101.

Article 706-102

The sound or audio-visual recordings are destroyed, at the initiative of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution.

An official record is made of the destruction.

2. Notion of organised crime and delinquency

Art. 706-73 lists the following felonies and misdemeanours under the Penal Code, unless otherwise stated in Title XXV of the Penal Procedure Code:

(1°) murder committed by an organised gang under 8° of article 221-4;

(2°) torture and acts of barbarity committed by an organised gang contrary to article 222-4;

(3°) felonies and misdemeanours relating to drug trafficking contrary to articles 222-34 to 222-40;

(4°) felonies and misdemeanours relating to kidnapping and false imprisonment committed by an organised gang contrary to article 224-5-2;

(5°) felonies and aggravated misdemeanours relating to human trafficking contrary to articles 225-4-2 to 225-4-7;

(6°) felonies and aggravated misdemeanours relating to procuring contrary to articles 225-7 to 225-12;

(7°) theft committed by an organised gang contrary to article 311-9;

(8°) aggravated felonies of extortion contrary to articles 312-6 and 312-7 ;

(9°) the felony of destroying, defacing or damaging property committed by an organised gang, contrary to article 322-8;

(10°) felonies relating to counterfeiting contrary to articles 442-1 and 442-2;

(11°) felonies and misdemeanours which constitute acts of terrorism contrary to articles 421-1 to 421-6;

(11° bis) felonies affecting the country's fundamental interests contrary to Title 1er of Book IV ;

(12°) misdemeanours relating to weapons and explosive materials contrary to articles 222-52 to 222-54, 222-56 to 222-59, 322-6-1 and 322-11-1, or contrary to articles L. 2339-2, L. 2339-3, L. 2339-10, L. 2341-4, L. 2353-4 and L. 2353-5 of the Code of defence, or contrary to articles L. 317-2 and L. 317-7 of the internal security Code;

(13°) misdemeanours in relation to the illegal entry, movement and residence of a foreigner in France committed by an organised gang, contrary to article L. 622-1 of the Code on the entry and residence for foreigners and on the right to asylum;

(14°) money laundering misdemeanours contrary to articles 324-1 and 324-2, or receiving stolen property contrary to articles 321-1 and 321-2, of the products, income and items resulting from the offences mentioned in 1° to 13°;

(15°) membership of a conspiracy misdemeanours contrary to article 450-1, where the action aims to prepare one of the penal infringements mentioned in 1° to 14° and 17°;

(16°) failure to justify resources corresponding to lifestyle misdemeanour contrary to article 321-6-1, when this misdemeanour is connected to one of the penal infringements listed in 1° to 15° and 17°;

(17°) crime of hijacking of aircraft, ships or any other means of transport committed by an organised gang under article 224-6-1;

(18°) crimes and misdemeanours sentenced to ten years of imprisonment contributing to proliferation of weapons of mass destruction and the means of delivering them under article 706-167;

(19°) misdemeanours of mining or licensable substance holding without an authorisation or exploitation permit, accompanied by damage to the environment, committed by an organised gang, contrary to article L. 512-2 of the mining Code, where it is related to one of the penal infringements mentioned in 1° to 17° of the current article;

(20°) Repealed (by law n°2017-1510 of 30 October 2017). (8° modified into 8bis) mentioned aggravated felonies of extortion contrary to articles 312-6 and 312-7, but this paragraph has been declared unconstitutional and was removed from the penal procedure Code on 1st September 2015 (see Decision n° 2014-420/421 QPC of the Constitutional Council of 9 Oct. 2014, recital n° 25).

Art. 706-73-1 lists the following felonies and misdemeanours under the Penal Code:

(1°) misdemeanour of fraud committed by an organised gang under the last paragraph of article 313-2; misdemeanour of violation of personal data processing operated by the State committed by an organised gang contrary to article 323-4-1 and misdemeanour of escape committed by an organised gang contrary to the second paragraph of article 434-30;

(2°) activities or employees concealment misdemeanour, misdemeanour of using the services of a person performing undeclared work, illegal subcontracting, illicit supply of workers, employment of foreign nationals without a work permit contrary to 1° and 3° of article L. 8221-1 and to articles L. 8221-3, L. 8221-5, L. 8224-1, L. 8224-2, L. 8231-1, L. 8234-1, L. 8234-2, L. 8241-1, L. 8243-1, L. 8243-2, L. 8251-1 and L. 8256-2 of the Labour Code;

(3°) money laundering misdemeanours contrary to article 324-1, or receiving stolen property contrary to articles 321-1 and 321-2, of the products, income and items resulting from the offences mentioned in 1° and 2° of the current article;

(3° bis) money laundering misdemeanours contrary to article 324-2, at the exception of those mentioned in 13° of article 706-73;

(4°) membership of a conspiracy misdemeanours contrary to article 450-1, where the action aims to prepare one of the penal infringements mentioned in 1° to 3° of the current article;

(5°) failure to justify resources corresponding to lifestyle misdemeanour contrary to article 321-6-1, when this misdemeanour is in link with one of the penal infringements listed in 1° to 4° of the current article;

(6°) misdemeanour of importing, of exporting, of transit, of transportation, of holding, of sale, of acquisition or of trade of a cultural good contrary to article 322-3-2;

(7°) misdemeanours of undermining the natural heritage committed by an organised gang contrary to article L. 415-6 of the Environmental Code;

(8°) misdemeanours of trafficking in plant protection products committed by an organised gang contrary to 3° of article L.253-17-1, to II of articles L. 253-15 and L. 253-16 and to III of article L. 254-12 of the Rural and Maritime Fishing Code;

(9°) Misdemeanours related to waste mentioned in I of article L. 541-46 of the Environmental Code committed by an organised gang, contrary to the VII of the same article;

(10°) Misdemeanour of participation in keeping a gambling house committed by an organised gang, contrary to the first paragraph of article L. 324-1 of the Internal Security Code, and misdemeanour of importation, of manufacture, of holding, of making available to third parties, of installation and of exploitation of gaming machines or of game of skills machines committed by an organised gang, contrary to the first paragraph of article L. 324-2 of the same code;

(11°) misdemeanours affecting the country's fundamental interests contrary to articles 411-5, 411-7 and 411-8, to the first two paragraphs of article 412-2, to article 413-1 and to the third paragraph of article 413-13.

C. Geolocation

Article 230-32

May be used any technical device aiming at locating in real-time, throughout the national territory, a person, a vehicle or any other object, without the consent of this person or the owner of this vehicle or object, where this measure is required for the needs:

– of an investigation or a judicial information related to a misdemeanour under Book II or under Articles 434-6[517] and 434-27[518] of the Penal Code, punishable by three years of imprisonment at least;

– of an investigation or a judicial information related to a felony or a misdemeanour, except those mentioned in the first paragraph of the current article, punishable by five years of imprisonment at least;

– of an investigation or a judicial information related to a death, a disappearance or an escape under articles 74, 74-1 and 80-4;

– of a search procedure related to an escaped person under article 74-2. from detention or to the provision of assistance to the author of a terrorism act, or related to a death, a disappearance or an escape[519]) according to articles 230-32 to 230-44 of the Penal Procedure Code.

Geolocation is implemented by a judicial police officer or, under his or her responsibility, by a judicial police agent, or it is prescribed by the judicial police officer, under the conditions and modalities provided for in the current Chapter.

Article 230-33

The operation mentioned in article 230-32 is authorised:

– Within the framework of a flagrancy investigation, of a preliminary investigation or of a procedure under articles 74 to 74-2, by the district prosecutor, for a maximal duration of 15 consecutive days. At the end of this period, this operation is authorised by the liberty and custody judge at the request of the district prosecutor, for a maximal duration of one month renewable under the same conditions of form and duration;

– Within the framework of a judicial information or of an information aiming to search for the causes of death or disappearance under articles 74, 74-1 and 80-4, by the investigating judge, for a maximal duration of four months renewable under the same conditions of form and duration.

The decision of the district prosecutor, of the liberty and custody judge and of the investigating judge is made in writing. It is not a jurisdictional decision and cannot be appealed.

Article 230-34

In situations mentioned in 1° and 2° of article 203-33, where the needs of the investigation call for it, the district prosecutor or the investigating judge may, on the sole purpose to implement or remove the technical device mentioned in article 230-32, authorise in writing the intrusion in private places aiming to or being used for the storage of vehicle, funds, commercial values or goods, including outside the visit times established in article 59, without the knowledge or consent of owner or occupant of these places or vehicles or of any other person having rights on the latter.

---

517 Art. 434-6 criminalises certain acts of assistance to the author or of the accomplice of a terrorist act.

518 Art. 434-27 criminalises escape.

519 Art. 230-32 PPC.

If this is a private place other than those mentioned in the first paragraph of the current article, this operation may only take place in situations described in 3° and 4° of article 230-32 or where the investigation or judicial information is related to a felony or a misdemeanour punishable by five years of imprisonment at least. If this private place is a home, the authorisation is delivered by the means of a written decision:

1° In situations provided for in the 1° of article 230-33, from the liberty and custody judge, requested to this end by the district prosecutor;

2° In situations provided for in the 2° of this same article 230-33, from the investigating judge or, where operations must take place outside the times mentioned in article 59, from the liberty and custody judge, requested to this end by the investigating judge.

The implementation of the technical device mentioned in article 230-32 cannot be made in places mentioned in articles 56-1 to 56-5, nor in the office or the home of persons mentioned in article 100-7.

Article 230-35

In situation of emergency resulting from an imminent risk targeting the integrity of evidence or an imminent risk of serious harm to people or goods, operations mentioned in article 230-32 may be implemented or prescribed by a judicial police officer. The latter must inform immediately, by any means, the district prosecutor or the investigating judge in situations mentioned in articles 230-33 and 230-34. This magistrate may then order the release of geolocation.

However, where the intrusion in a home is necessary, the judicial police officer must gain the prior agreement, given by any means:

1° In situations provided for in the 1° of article 230-33, from the liberty and custody judge, requested to this end by the district prosecutor;

2° In situations provided for in the 2° of this same article 230-33, from the investigating judge or, where operations must take place outside the times mentioned in article 59, from the liberty and custody judge, requested to this end by the investigating judge.

These magistrates are granted with a 24 hours delay in order to prescribe, by means of a written decision, the continuance of operations. Failing that, the geolocation is stopped. In situations provided for in the first paragraph of the current article, the authorisation includes a statement on the circumstances in fact that establish the existence of the imminent risk mentioned in this same paragraph.

Article 230-36

The investigating judge or the judicial police officer assigned by the latter or authorised by the district prosecutor may require any qualified agent of a service, of a unit or of a body placed under the authority of the Ministry of the Interior, the list of which is set by decree, with a view to proceeding with the implementation and the removal of the technical device mentioned in article 230-32.

Article 230-37

Operations provided for in the current chapter are conducted under the supervision of the magistrate who authorised them or who authorised their prolongation.

The fact that these operations reveal penal infringements other than those mentioned in this magistrate's decision is not a cause for nullity of incidental proceedings.

Article 230-38

The judicial police officer or the judicial police agent who acts under his responsibility establishes an official record of each of operations of implementation of the technical device mentioned in article 230-32 and of operations of registration of location data. This official record mentions the date and time at which operation began and ended.

Recordings are placed under closed seals.

Article 230-39

The judicial police officer or the judicial police agent who acts under his responsibility transcribes, in an official record which is added to the case file, the registered data that are useful to ascertain the truth.

Article 230-40

Where, within the framework of a judicial information related to a felony or a misdemeanour covered by the scope of application of articles 706-73 and 706-73-1[520], the release of this information is likely to seriously harm the life or the physical integrity of a person, of his or her family members or of his or her relatives, while this information is neither useful to ascertain the truth, nor essential to the exercise of the rights of defence, the liberty and custody judge, seized at any moment by a reasoned request from the investigating judge, may, by the means of a reasoned decision, authorise that do not appear in the case file:

1° The date, time and place where the technical device mentioned in article 230-32 has been implemented or removed;

2° The record of location data and elements that enable to identify a person who has contributed to the implementation or to the removal of the technical device mentioned in this same article;

The decision of the liberty and custody judge mentioned in the first paragraph of the current article is joined to the case file. Information mentioned in the 1° and the 2° are recorded in another official record, which is kept in a separate file, different from the case file, in which is also included the request from the investigating judge provided for in the first paragraph. This information is recorded in a numbered and signed register, which is created to this end at the district court[521].

Article 230-41

The accused person or the witness to be assisted may, within ten days from the date at which he or she has been made aware of the geolocation operations executed within the framework provided for in article 230-40, contest, before the president of the investigating chamber, the recourse to the procedure provided for in this same article. Where he or she considers that geolocation operations were not executed in accordance with the proper process, that the requirements set out in the same article are not fulfil or that information mentioned in this same article are essential to the exercise of the rights of defence, the president of the investigating chamber orders the cancellation of the geolocation. However, if he or she considers that the release of the information is not or is not any more likely to seriously harm the life or the physical integrity of a person, of his or her family members or of his or her relatives, he may also order the insertion in the case file of the request and of the official record mentioned in the first paragraph of this same article. The president of the investigating chamber makes his or her decision by way of reasoned order, which cannot be appealed, on the basis of documents relevant to the proceedings and of documents included in the file mentioned in the same paragraph.

Article 230-42

No verdict shall be based on information collected under the conditions provided for in article 230-40, unless where the request and the official record mentioned in the last paragraph of this same article have been added to the case file by application of article 230-41.

---

520 See above, Appendix, Section B.2.

521 The Tribunal de grande instance.

Article 230-43

Recordings of location data are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution.

An official record is made of the destruction.

Article 230-44

The current chapter is not applicable where real-time geolocation operations aim at locating an electronic communication terminal equipment, a vehicle or any other object whose owner or legitimate possessor is the victim of the penal infringement which is the object of the investigation or of the judicial information, or is the disappeared person in the meaning of articles 74-1 or 80-4, as long as these operations aim to find the victim, the object that has been stolen to him or her or the disappeared person.

In situations provided for in the current article, real-time geolocation operations are the object of requisitions in compliance with articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3 or 99-4[522] of the Penal Procedure Code.

D. Interception of the Content of the Information Accessed by Users of Electronic Communications Operators' Services

The interception of the content of the information accessed by users of electronic communications operators' services is set out in articles 60-2 (flagrancy investigation), 77-1-2 (preliminary investigation), and 99-4 (judicial investigation, which means investigation procedure conducted by an investigating judge) PPC.

Article 60-2, §2 *et seq*.

A judicial police officer, acting upon orders of a district prosecutor authorised in advance by an order from the liberty and custody judge, may require telecommunications operators, particularly those mentioned in 1 of I of article 6 of Law no. 2004-575 of 21 June 2004 relating to confidence in the digital economy,[523] to take without delay all appropriate measures to ensure the preservation, for a period that may not exceed one year, of the content of the information accessed by persons using the services provided by the operators.

The organisations or persons to which this article applies must make the required information available as quickly as possible by means of telecommunication or computers.

Refusal to respond to such a request without a legitimate reason is punished by a fine of €3750.

[…]

Article 77-1-2, §2 *et seq*.

On the authorisation of the liberty and custody judge, seized to this end by the district prosecutor, a police officer may carry out the measures provided for in the second paragraph of article 60-2.

The organisations or persons concerned make the required information available as quickly as possible, by means of telecommunication or computers.

---

522 See above, Section III.C.1.

523 These persons are Internet access service providers.

Refusal to respond to such a request without a legitimate reason is punished subject to the provisions of the fourth paragraph of article 60-2.

Article 99-4, §2 *et seq*.

With the express permission of the investigating judge, a judicial police officer may issue the demands provided for in the second paragraph of article 60-2.

The organisations or persons concerned must put the requisite information at their disposal by telecommunication or by use of computers as quickly as possible.

Refusal to respond to these demands without legitimate grounds is punished in accordance with the provisions of the fourth paragraph of article 60-2.

E. Mutual Legal Assistance

1. General provisions

Article 694[524]

In the absence of any international conventions stipulating otherwise:

1° Requests for mutual assistance coming from French judicial authorities and addressed to foreign judicial authorities are sent through the intermediary of the Minister of Justice. The enforcement documents are sent to the authorities of the requesting State through the same channels.

2° Requests for judicial assistance coming from foreign judicial authorities are sent through diplomatic channels. The enforcement documents are sent to the authorities of the requesting State through the same channels.

In urgent cases, requests for mutual assistance sought by the French or foreign authorities may be directly sent to the authorities of the State who are competent to enforce them. The transmission of the enforcement documents to the authorities of the requested State is carried out in the same way and under the same conditions. However, unless there is an international convention stipulating otherwise, requests for judicial assistance coming from foreign judicial authorities and addressed to the French judicial authorities must be the subject of an opinion sent through diplomatic channels by the foreign government concerned.

Article 694-1

In urgent cases, requests for judicial assistance coming from foreign judicial authorities are sent, according to the distinctions set out in article 694-2, to the district prosecutor or the investigating judge of the territorially competent district court. They may also be sent to these judges through the intermediary of the prosecutor general.

If the district prosecutor receives a request for judicial assistance directly from a foreign authority which m s. PPCay only be executed by the investigating judge, he sends it to the latter to be carried out, or seizes the prosecutor general in the case provided for in article 694-4.

Before executing a request for judicial assistance of which he has directly be seized, the investigating judge immediately sends this to the district prosecutor for his opinion.

---

[524] See the English translation of the French Penal Procedure Code proposed by Legifrance at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf (arts. 694 to 694-4 in this document correspond to their current version. Further articles have mostly been modified since the translation has been done).

Article 694-2

Requests for judicial assistance coming from foreign judicial authorities are executed by the district prosecutor or by judicial police officers or agents nominated for this purpose by this prosecutor.

They are executed by the investigating judge or judicial police officers acting in the context of a rogatory letter where they require particular procedural acts which may not be ordered or executed in the course of a preparatory investigation.

Article 694-3

Requests for judicial assistance coming from foreign judicial authorities are executed according to the procedural rules provided for by the present Code.

However, if the request for judicial assistance specifies this, it is executed in accordance with the procedural rules indicated by the competent authorities of the requesting State, on the condition, under penalty of nullity, that these rules do not reduce the rights of the parties or the procedural guarantees provided for by the present Code. Where the request for judicial assistance may not be executed in accordance with the stipulations of the requesting State, the competent French authorities immediately inform the authorities of the requesting State and indicate under which conditions the request may be executed. The competent French authorities and those of the requesting State may agree on the outcome of this request later on, where appropriate by subjecting it to the aforesaid conditions.

The irregularity of the sending of the request for judicial assistance may not constitute grounds for nullity of the acts executed in enforcing this request.

Article 694-4

If the enforcement of a request for judicial assistance coming from a foreign judicial authority is liable to threaten public order or the fundamental interests of the nation, the district prosecutor seized of this request in accordance with the third paragraph of article 694-1 sends this to the prosecutor general who decides, if appropriate, to seize the Minister of Justice and gives, where applicable, notice of this reference to the investigating judge.

If he is seized, the Minister of Justice informs the authority which made the request, if appropriate, that no action, total or partial, may be taken in relation to the request. This information is communicated to the judicial authority concerned and blocks the enforcement of the request for judicial assistance or the return of the enforcement documents.

Article 694-4-1

If a request for assistance issued by a foreign authority is related to facts committed outside the national territory likely to be linked to missions executed by an intelligence service provided for by article L811-2 of the Internal Security Code, for the purpose of promotion and defence of the nation fundamental interests under article L. 811-3 of the Internal Security Code, the district prosecutor who is seized with the request or who is informed of it in application of article 694-1 of the Penal Procedure Code transmits this request to the district prosecutor who in turn must seize the Minister of Justice and inform on this transmission, if appropriate, the investigating judge.

The Minister of Justice informs the minister who supervises the specialised intelligence service which is concerned and takes its opinion.

Within one month, the latter inform the Minister of Justice on the fact that the execution of the request for assistance is or not likely to harm the fundamental interests of the State.

The Ministry of Justice informs the requesting authority, if appropriate, that no action, total or partial, may be taken in relation to the request. This information is communicated to the judicial authority concerned and blocks the enforcement of the request for judicial assistance or the return of the enforcement documents.

2. European investigations orders

Article 694-14

Provision of this chapter are applicable to request for assistance between France and other Member States of the European Union.

Articles 694-15 to 694-50 are related to European investigations orders and implement Directive 2014/41/UE of 3 April 2014.

3. Joint investigation teams

Article 695-2

Where there is need to carry out, in the context of a French prosecution, either complex inquiries involving the mobilisation of extensive resources and which concern other member states or where several member states are carrying out inquiries into offences which call for coordinated and concerted action between the member states concerned, with the prior agreement of the Minister of Justice and the consent of the member state or states concerned, the competent judicial authority may create a joint investigation team.

Foreign agents seconded by another member state to a joint investigation team may, within the limits of the powers conferred on them by their role, and under the supervision of the competent judicial authorities, have as their mission, as appropriate, over the whole of the national territory:

1° the establishment of any felonies, misdemeanours or petty offences, and to record these in an official record, if necessary in the forms provided for by the law of their state;

2° the reception of the official reports of any statements made to them by any person liable to provide information on the facts in question, if necessary in the forms provided for by the law of their state;

3° the secondment of French judicial police officers in the exercise of their duties;

4° the carrying out of any surveillance and, if they are authorised for this purpose, infiltration, under the conditions provided for in articles 706-81 onwards, and which is necessary for the application of articles 694-7 and 694-8.

Foreign officers attached to a joint investigation team may carry out these missions subject to the consent of the member state which has implemented their secondment.

These officers may only carry out the operations for which they have been designated. None of the powers which are the preserve of the French judicial police officer who is in charge of the team may be delegated to them.

The original copy of the official records which they prepare, and which must be drafted or translated into French, is attached to the case file.

Article 695-3

In the context of a joint investigation team, French judicial police officers and agents attached to a joint investigation team may carry out operations ordered by the head of the

team, over the whole of the territory of the State in which they are operating, within the limit of the powers conferred on them by the present Code.

Their tasks are defined by the authorities of the Member State competent to direct the joint investigation team in the territory where the team is working.

They may receive statements and record offences in the forms provided for by the present Code, subject to the consent of the State in whose territory they are operating.

4. Simplified exchange of information

General provisions - articles 695-9-31 and 695-9-32

Article 695-9-31 authorises National police and gendarmerie services and certain custom, finance and Ministry of the Interior's services to exchange, with competent services of another Member State, information that is at their disposal, in the aim of preventing a penal infringement, of collecting evidence in relation with a penal infringement or of searching for perpetrators of a penal infringement, either they detain it or they can access it, especially through the consultation of a data processing system, without making it necessary to take or ask for a requisition measure or another coercive measure.

Article 695-9-32 sets out that exchanged information is confidential, which must be guaranteed by its means of transmission and of storage.

Request for information issued by French services - articles 695-9-33 to 695-9-36

When reasons exist to assume that a Member state holds information described in article 695-9-31 that is useful in order to prevent a penal infringement, or that is useful to investigations aiming at establishing evidence of a penal infringement or to search for its perpetrators, services and units mentioned in article 695-9-31 may request the transmission of this information from the relevant services of this State. The request for transmission must provide the reasons on which they base their assumption that this information is in the possession of these services, and must mention the purposes of the request for information, and, when this information is related to an identified individual, it must mention the link between this person and the purposes of the request (article 695-9-33).

Obtained information cannot be used as evidence without the agreement of the Member State that has transmitted it (article 695-9-34). This information cannot be used for other purposes (purposes other than those mentioned in the request) without the agreement of the Member State that has transmitted it, unless they may prevent a clear and immediate danger for public security (article 695-9-35). These provisions do not prevent the possibility for relevant authorities to control the modalities of processing and storage of transmitted information (article 695-9-35). If the transmitting State asks for it, the service or unit that obtained the information informs the relevant service of this State about the use that has been made of this information (article 695-9-36).

Request for information received by French services - articles 695-9-37 to 695-9-47

Services and units mentioned in article 695-9-31 transmit, when requested so by relevant services of an EU member State, the information mentioned in the same article and that is useful in order to prevent a penal infringement, or that is useful to investigations aiming at establishing evidence of a penal infringement or to search for its perpetrators (article 695-9-37).

If the information mentioned in article 695-9-31 may be useful to another Member State to prevent one of the penal infringements mentioned in article 695-32[525] and punished by at least three years of imprisonment, or if this information may be useful to this other member State in order to conduct investigations aiming at establishing evidence of such a penal infringement or to search for its perpetrators, the service or unit that holds this information transmits it to this other Member State without the need of having received a corresponding request (article 695-9-38[526]).

When this information is initially transmitted by another Member State on the basis of the framework decision 2006/960/JAI, it may only be transmitted to another Member State following the conditions imposed by the first transmitting Member State. When this information is initially transmitted by another Member State on a basis other than the framework decision 2006/960/JAI, or by a non-EU Member State, it may only be transmitted to another Member State with the agreement of the first transmitting State and under the conditions imposed by this State, in all the situations where France must respect these principles according to an International agreement (article 695-9-39).

Information can only be transmitted, to the relevant services of the Member State that requested it, with the authorisation of a judge, each time such an authorisation is mandatory under French law in order to access this same information or to transmit this same information to a judicial police service or unit. The request for authorisation is addressed to the relevant judge by the service or unit to which the information is requested. Elements of an ongoing penal procedure can only be transmitted with the authorisation of the investigating court in charge of the case, or with the authorisation of the district prosecutor when the trial court has been seized (article 695-9-40).

Services or units mentioned in article 695-9-31 cannot refuse to communicate information requested by a Member State, unless reasons exist to think that such communication:

– could be prejudicial to the fundamental interests of the State in terms of National security;
– could be prejudicial to ongoing investigations in penal matters or would jeopardise people's security;
– or would be clearly disproportionate or pointless in relation to the purposes for which the information has been requested (article 695-9-41).

Services or units mentioned in article 695-9-31 may refuse to transmit requested information when it relates to a penal infringement punished in France by a year or less of imprisonment and when they consider that the information is not of sufficient interest to justify the constraints attached to its transmission (article 695-9-42).

On the occasion of the transmission of the information, the service or unit mentioned in article 695-9-31 indicates to the receiving service the conditions of use of the information. Each time it deems it is necessary, it may ask the receiving service to provide information about the use that has been made of the transmitted information (article 695-9-43).

Where information has been transmitted by a service or unit mentioned in article 695-9-31 to the relevant service of a Member State and where the latter considers transmitting it to another State or using it for another purpose than the one for which the transmission was permitted, the service or unit that made the original transmission is competent to consider

---

[525] Art. 695-32 lists several penal infringements including (non-exhaustively) participation in a criminal organisation, terrorism, human trafficking, child pornography and sexual exploitation of children, cybercrime.

[526] Modified by Ordinance n° 2016-1636.

whether the new transmission or the new use should be authorised, on the request of the receiving State, and, if needed, to determine the conditions of it (article 695-9-44).

Information transmitted by the service or unit mentioned in article 695-9-31 may be used by the receiving service as evidence, unless it was otherwise stipulated on the occasion of its transmission (article 695-9-45).

Information transmitted by the service or unit mentioned in article 695-9-31 to the relevant service of a Member State is also transmitted to the Eurojust and Europol units, to the extent it relates to a penal infringement falling within their mandate (article 695-9-46).

Contact points to whose requests for transmission of information can be addressed by relevant services of Member States are nominated by order of the Ministry of Justice, of the Ministry of the Interior and of the Ministry responsible for the budget (article 695-9-47).

Modalities of application or articles 695-9-31 to 695-9-47 are determined by a Decree issued by the Council of State (article 695-9-49).

Application of previous provisions to certain States that are not members of the European Union (articles 695-9-48 and 695-9-49)

Articles 695-9-31 to 695-9-47 are applicable to the exchange of information mentioned in article 695-9-31 between services and units mentioned in the latter article and relevant services from States which are not members of the EU but which are associated with the implementation, the application and the development of the Schengen *acquis* (article 695-9-48).

Modalities of application are determined by a Decree issued by the Council of State (article 695-9-49).

Bibliography*

Andriantsimbazovina, Joël, "Ouverture: l'extériorisation de la prise en compte de la Convention européenne des droits de l'homme", in "La prise en compte de la Convention européenne des droits de l'homme par le Conseil constitutionnel, continuité ou évolution ?", Cahiers du Conseil constitutionnel n° 18 (Dossier: Constitution et Europe) – July 2005, https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-prise-en-compte-de-la-convention-europeenne-des-droits-de-l-homme-par-le-conseil-constitutionnel

Beaume, Jacques, Rapport sur la procédure pénale, July 2014, p. 43, available at http://www.justice.gouv.fr/publication/rap-beaume-2014.pdf

Cahn, Olivier, "Un Etat de droit, apparemment …" (A State under the rule of law, apparently …), AJ Penal, 2016, p. 201.

Chefs d'institution de l'Association des Cours constitutionnelles ayant en partage l'usage du français, "La proportionnalité dans la jurisprudence constitutionnelle," 5ème conférence, 8–13 July 2008, p. 7, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/Bilan_2008/confV_accpuf_libreville_juillet2008.pdf

* All URLs were last accessed in February 2019.

Commission nationale de contrôle des interceptions de sécurité, CNCIS, report for the years 2013–2014, http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000101.pdf

Cour de cassation, rapport annuel 2012, *La preuve*, Livre 3, partie 4, Titre 2, Chapitre 2 – Admissibilité des modes de preuve, available at https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2012_4571/livre_3_etude_preuve_4578/partie_4_administration_preuve_4589/principes_gouvernant_4591/admissibilite_modes_26241.html

Daoud, Emmanuel, "Le point de vue d'un avocat" (The point of view of an advocate), in Katarzyna Blay-Grabarczyk and Laure Milano (dir.), Lutte contre le terrorisme et droits fondamentaux (The combat against terrorism facing fundamental rights), Institut Universitaire Varenne, coll. "Colloques et Essais," L.G.D.J. – Lextenso, 3rd trim. 2017, pp. 171–183.

De Marco, Estelle, "La captation des données" (Data capture), in Katarzyna Blay-Grabarczyk and Laure Milano (dir.), *Lutte contre le terrorisme et droits fondamentaux* (The combat against terrorism facing fundamental rights), Institut Universitaire Varenne, coll. "Colloques et Essais," L.G.D.J. – Lextenso, 3rd trim. 2017, pp. 91–107.

– *Comparative study between Directive 95/46/EC and the GDPR including their relations to fundamental rights*, March 2018, Deliverable D2.10, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/

– (ed.), *Identification and analysis of the legal and ethical framework*, July 2017, Deliverable D2.2, MANDOLA EU project, GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications/

– "Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux," 4 June 2009, Juriscom.net, http://www.juriscom.net/uni/visu.php?ID=1133

– *L'anonymat sur Internet et le droit*. Thesis, Montpellier 1, 2005, ANRT.

De Marco, Estelle/Callanan, Cormac, in: C. Callanan/M. Gercke/E. De Marco/H. Dries-Ziekenheiner, *Internet blocking – balancing cybercrime responses in democratic societies*, October 2009, n° 6.5.2.2, available at http://www.aconite.com/blocking/study (French version available at http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/)

Dutheillet de Lamothe, Olivier, "L'influence de la Cour européenne des droits de l'Homme sur le Conseil constitutionnel, 13 février 2009, Conseil constitutionnel, visite du Président et d'une délégation de la Cour européenne des droits de l'homme au Conseil constitutionnel, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/pdf/Conseil/cedh_130209_odutheillet.pdf

Goesel-Le Bihan, Valérie, "Le contrôle de proportionalité exercé par le Conseil constitutionnel, technique de protection des libertés publiques?", http://juspoliticum.com/Le-controle-de-proportionnalite.html

Kayser, Pierre, *La protection de la vie privée par le droit*. 3rd ed. PU d'Aix-Marseille/Economica 1995.

Lafay, Frédérique, note under Decision of the Constitutional Council n° 94-352 DC, 18 January 1995, J.O. 21 January 1995, p. 1154 and JCP 1995, II, 22525.

Lemoine, Pascal, "La loyauté de la preuve (à travers quelques arrêts récents de la chambre criminelle)," Cour de cassation annual report 2004, available at https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2004_173/deuxieme_partie_tudes_documents_176/tudes_diverses_179/travers_quelques_6401.html.

Mazeaud, Vincent, "La constitutionnalisation du droit au respect de la vie privée" (the constitutionalisation of the right to respect for private life), nouveaux cahiers du Conseil constitutionnel n°48 (dossier vie privée), June 2015, available at https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-constitutionnalisation-du-droit-au-respect-de-la-vie-privee#ref-note-25

Peltier, Virginie, *Le secret des correspondances*. PU d'Aix-Marseille 1999.

Rassat, Michèle-Laure, note under Cass. crim., 15 June 1993: bull. crim., n° 210. 6 April 1993, JCP 1993, II, 22144.

– note under Cass. crim., 27 February 1996, "Schuller" court case, bull. crim. 1996, n° 93; JCP 1996, ed. G, II, 22629.

Robert, Jacques/Duffar, Jean, *Droits de l'homme et libertés fondamentales*. 7th ed. Montchrestien 1999, p. 27.

Sudre, Frédéric, "La dimension internationale et européenne des libertés et droits fondamentaux" in: Rémy Cabrillac/Marie-Anne Frison-Roche/Thierry Revet (dir.), *Libertés et droits fondamentaux*. 11th ed. Dalloz 2005.

List of Abbreviations

bull. crim.	Bulletin de la Cour de Cassation, chambre criminelle (reports of the Court of Cassation's decisions, criminal chamber)
CA	Cour d'appel
Cass. crim.	Cour de cassation, chambre criminelle (Criminal Chamber of the Court of Cassation)
CC	Civil Code
CNCIS	Commission nationale de contrôle des interceptions de sécurité (National Commission for the Control of Security Interceptions)
CNCTR	Commission nationale de contrôle des techniques de renseignement (National Commission for the Control of Intelligence Techniques)
D.	Recueil Dalloz (law journal)
dir.	sous la direction (edited by)
DJS	Droits, Justice et Sécurités (laws, justice, and securities)

ECtHR	European Court of Human Rights
ECHR	European Convention on Human Rights
IP	Internet Protocol
ISC	Internal Security Code
JCP	La semaine juridique (law journal)
JCP. ed. G	La semaine juridique édition génerale (law journal, general edition)
J.O.	Journal Officiel (Official Gazette of the French Republic)
JORF	Journal officiel de la République française (Official Gazette of the French Republic)
PC	Penal Code
PECC	Post and Electronic Communications Code
PPC	Penal Procedure Code

Ulrich Sieber / Nicolas von zur Mühlen / Tatiana Tropina (eds.)

Access to Telecommunication Data in Criminal Justice

Schriftenreihe des Max-Planck-Instituts für
ausländisches und internationales Strafrecht

Strafrechtliche Forschungsberichte

Herausgegeben von Ulrich Sieber

Band S 156.2

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Access to Telecommunication Data in Criminal Justice

A Comparative Legal Analysis

2nd revised and expanded edition

Ulrich Sieber • Nicolas von zur Mühlen
Tatiana Tropina (eds.)

Volume 2

Duncker & Humblot • Berlin

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten
© 2021 Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.
c/o Max-Planck-Institut für ausländisches und internationales Strafrecht
Günterstalstraße 73, 79100 Freiburg i.Br.
http://www.mpicc.de
Vertrieb in Gemeinschaft mit Duncker & Humblot GmbH, Berlin
http://www.duncker-humblot.de

Umschlagbild: © istock.com/kynny
Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim
Printed in Germany
Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706

ISSN 1860-0093
ISBN 978-3-86113-767-2 (Max-Planck-Institut)
ISBN 978-3-428-18272-5 (Duncker & Humblot)
DOI unter https://doi.org/10.30709/978-3-86113-767-2
CC-Lizenz by-nc-nd/3.0

Preface

Access to telecommunication data is an essential and powerful investigative tool in criminal justice. At the same time, the interception of such data can seriously affect individual privacy. This is true not only with respect to content data but with respect to traffic data as well. The legal instruments and provisions that allow the gathering of these data are primarily the traditional rules on the interception of telecommunication based on the cooperation duties of telecommunication providers. In addition, access to telecommunication data can also be granted by rules on remote forensic software, by search and seizure of – temporarily or permanently – stored data, and (esp. in cases of traffic and subscriber data) by production orders demanding the delivery of stored data.

The rules governing these interception techniques vary considerably among the national legal orders. Differences are found, for example, in the formal requirements for interception orders, in the scope of professional secrecy and privacy protections leading to the exemption from interception, and in the possibilities to access (esp. encrypted) telecommunication data by means of remote forensic software, either to specifically procure telecommunication data or in general. These legal differences are not only most interesting from the perspective of fundamental research in the area of comparative criminal law but also for practical reasons, such as identifying best practices and evaluating the scope of international cooperation.

This publication provides a comparative analysis dealing with the commonalities and differences of these rules on interception and other means of access to telecommunication data. It also includes country reports on the following legal orders on which this comparison is based: Australia, Austria, Belgium, Croatia, the Czech Republic and Slovakia, Estonia, France, Germany, Hungary, Italy, the Netherlands, Poland, Portugal, Spain, Sweden, the Untited Kingdom, and the United States of America. The research undertaken on these countries encompasses not only the law on the books but also the law in action as analyzed in interviews and workshops with specialists in the fields of telecommunication interception and international cooperation in criminal matters. The analysis of law in action also includes Switzerland, in addition to the above-mentioned countries.

The original incentive to conduct this analysis was an expert opinion prepared for the German Central Office for Information Technology in the Security Sector (ZITiS) on international cooperation in the interception of telecommunication. International cooperation in this area based on mutual legal assistance was and still is complicated, slow, and – in practice – rare. For these reasons, the goal of the study

for the ZITiS was to develop legal and technical solutions by means of which telecommunication data could be transmitted from one country to another in real time, by direct transmission, and without violating human rights standards. Since such transmissions are especially problematic due to differences in the laws of the various national orders (esp. professional secrecy and privacy protections), the study also required a specific comparative analysis of these differences. The solutions developed for ZITiS on international cooperation was published in a separate volume (S 157 of this book series) in German.

The wealth of information gathered by this practice-oriented study on international cooperation inspired us to develop our applied research into a general comparative analysis on access to telecommunication data, which is published in this book. In contrast to the above-mentioned study for the ZITiS, this general comparative analysis is written in English and addresses not only questions that arise in the context of mutual legal assistance in interception of content data but rather covers all questions implicated in the context of access to telecommunication data. Thus, the scope of this second study extends beyond traditional interception and includes all types of access to telecommunication data that can be used as functional equivalents to traditional interception. Additionally, it is not limited to the interception of content data but rather covers access to traffic and subscriber data as well. In contrast to the above-mentioned study, this publication contains both the results of the comparative study as well as the underlying country reports. As a consequence, the general analysis on access to telecommunication data presented here not only supports our specific study on legal cooperation in interception but can also serve as a general research tool in support of future studies and practical work.

We would like to thank both the academic authors of the country reports for their most valuable support of this study and the many dedicated practitioners who provided us with comprehensive, detailed information about the concrete situation in their countries in interviews in Brussels, Budapest, Gießen, Lisbon, London, Madrid, Paris, Prague, Rome, Stockholm, Tallinn, Utrecht, Vienna, and Zurich. Above all, we are most grateful to Mr. *Christian Förster* from ZITiS as the appointed project manager, who efficiently organized and made possible these interviews on "the law in action." In addition, sincere thanks are also due to our editing and proofreading teams, especially Ms. *Petra Lehser*, Ms. *Indira Tie*, and Ms. *Anna Riddell* (as external proofreader).

Freiburg, March 2021

Prof. Dr. Dr. h.c. mult. *Ulrich Sieber*
Dr. *Nicolas von zur Mühlen*
Dr. *Tatiana Tropina*

Contents

Germany*

National Rapporteurs:
Benjamin Vogel
Patrick Köppen
*Thomas Wahl***

* This report reflects legislation and case law as of November 2019.

** Benjamin Vogel (Sections I.–III.B.); Patrick Köppen (Sections III.C.–IV.); Thomas Wahl (Section V.); Sections I.–IV. translated by Daniel Burke.

Contents

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Security Services with Powers of Telecommunication Interception

1. National security architecture

In Germany, the prevention and prosecution of crime is handled by various authorities. The focus lies upon the repressive tasks of public prosecutors, who are declared competent for criminal prosecution by the Code of Criminal Procedure (*Strafprozessordnung*, StPO), and the police authorities supporting them.

Additionally, police authorities are charged with the preventive task of averting danger, as stipulated in the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz*, BKAG), the Federal Police Act *(Bundespolizeigesetz)* and the Police Acts of the *Länder* (the *Länder* being the 16 states of the Federal Republic of Germany) *(Landespolizeigesetze)*. The Federal Criminal Police Office *(Bundeskriminalamt)* supports public prosecutors in law enforcement activities involving certain forms of serious crime and is responsible for the aversion of dangers connected with international terrorism. The Federal Police *(Bundespolizei)* is competent for averting danger particularly in the fields of border protection, the safety of railway facilities, and aviation security. It is also responsible for the investigation of certain offences connected with its preventive duties. For all other areas, the police authorities of the *Länder* are charged with averting danger and assisting public prosecutors in their law enforcement activities.

The tasks of intelligence agencies also belong to the field of prevention. Concerning state security (and in some *Länder*, also concerning organised crime) the Federal (*Bundesamt für Verfassungsschutz*, BfV) and State Offices for the Protection of the Constitution *(Verfassungsschutzämter der Länder)* are entrusted with collecting and analysing information. Pursuant to the Act on the Federal Intelligence Service (*Gesetz über den Bundesnachrichtendienst*, BNDG), the Federal Intelligence Service (*Bundesnachrichtendienst*, BND) gathers information of relevance to foreign and security policy, thus functioning as a foreign intelligence service. In individual cases, the Federal Intelligence Service may also take action to protect the health or life of a person in a foreign country. In the Federal Ministry of Defence's area of responsibility, the collection and analysis of information critical to state security is carried out by the Military Counterintelligence Service (*Militärischer Abschirmdienst*, MAD).

The Customs Criminal Office *(Zollkriminalamt)* and the Customs Investigation Offices *(Zollfahndungsämter)* are charged with monitoring foreign trade and the cross-border movement of goods. According to the Customs Investigation Act *(Gesetz über das Zollkriminalamt und die Zollfahndungsämter)*, their activities in this field include tasks of both preventive and repressive nature – the latter involves giving support to public prosecutors in criminal prosecution. In order to detect the commission of customs-related offences, the Customs Criminal Office continually monitors the internal and transnational movement of goods, capital, and services.

2. Powers for the interception of telecommunication

a) Law of criminal procedure

Pursuant to Section 100a StPO, the prosecution authorities are authorised to intercept telecommunication. This requires in particular the suspicion – based on specific facts – that certain serious offences have already been committed. The order must be given or confirmed by a judge.

b) Preventive law

Moreover, the interception of the content of telecommunication is permitted for preventive purposes according to Section 51 BKAG and the police laws of most *Länder*. As a prerequisite, this generally requires a danger threatening the existence or security of the state, the life, health, or liberty of a person, or property of substantial value.[1] Suspicion of preparing particularly serious crimes, such as terrorist offences or violations of the War Weapons Control Act *(Kriegswaffenkontrollgesetz)*, also grants some police authorities the power to intercept telecommunication.[2] Such suspicion must be based on the existence of facts. Finally, the preventive interception of telecommunication is not exempt from the requirement of a judicial order or confirmation. Likewise, telecommunication providers' duties of information disclosure concerning traffic and subscriber data are stipulated explicitly in Section 20m BKAG and the police laws of most *Länder*.[3] Furthermore, the Federal Criminal Police Office is authorised to perform clandestine intrusions into information systems pursuant to Section 20k BKAG, as well as to employ IMSI-catchers for determining the location of active mobile terminal devices or for determining device or card numbers pursuant to Section 20n BKAG.

---

[1] Section 51 Subsection 1 BKAG and, e.g., Article 42 Subsection 1 BayPAG; Section 10b Subsection 1 HamDVPolG; Section 15a Subsection 1 HSOG; cp. *Schenke*, Polizei- und Ordnungsrecht, 2013, pp. 122 et seq.

[2] See Section 20l Subsection 1 Sentence 1 No. 2 in connection with Section 4a Subsection 1 Sentence 2 BKAG; Section 33b Subsection 1 BbgPolG.

[3] Section 20m BKAG and, e.g., Section 23a BWPolG; Article 43 BayPAG; Section 15a Subsection 2 and 2a HSOG; see *Schenke*, Polizei- und Ordnungsrecht, pp. 125 et seq.

c) Law of intelligence agencies

As laid down in Section 1 Subsection 1 No. 1 in connection with Section 3 Subsection 1 of the Act Restricting the Secrecy of the Post, of Letters, and of Telecommunication (*Gesetz zur Beschränkung des Post-, Brief- und Fernmeldegeheimnisses*, G 10), the Federal and State Offices for the Protection of the Constitution, the Military Counterintelligence Service, and the Federal Intelligence Service are authorised to monitor the communication of individual connections for the purpose of averting danger threatening the free democratic basic order or the existence or security of Germany or its *Länder*. This requires that someone is under suspicion of planning, committing, or having committed offences pertaining to state security (so-called telecommunication interception in the individual case). In this case, the order to execute the measure is not given by a judge but by the Federal Ministry of the Interior or the competent state ministry, as the case may be. Furthermore – and in contrast to the powers of criminal procedure – establishing suspicion requires only mere factual indications. According to Section 8 G 10, the Federal Intelligence Service may, in individual cases, also intercept international telecommunication in order to protect a person in a foreign country from imminent danger to life or health.

Section 1 Subsection 1 No. 2 in connection with Section 5 G 10 allows the Federal Intelligence Service to monitor international telecommunication by utilising search terms in order to collect information relating to certain forms of serious transnational crime; it may do this without existing suspicion[4] (so-called strategic telecommunication interception). However, the measure may not lead to the deliberate surveillance of a domestic telecommunication connection.

With the Counter-Terrorism Act of 2002 *(Terrorismusbekämpfungsgesetz)*, the Federal Office for the Protection of the Constitution, the Federal Intelligence Service, and the Military Counterintelligence Service were granted the power to gather customer and user-related information from telecommunication and teleservice companies in individual cases, and to use IMSI-catchers for determining the location of an active mobile terminal device or for determining the device or card number (Section 8a Subsection 2 Sentence 1 No. 4, 5 and Section 9 Subsection 4 of the Federal Constitutional Protection Act, *Bundesverfassungsschutzgesetz*, BVerfSchG); Section 3 Subsection 1 and Section 5 BNDG; Section 4a Sentence 1 and Section 5 of the Military Counterintelligence Service Act (*Gesetz über den militärischen Abschirmdienst*, MADG). The requests for information must be applied for in writing at the Federal Ministry of the Interior (for the Federal Office for the Protection of the Constitution), the Federal Chancellery (for the Federal Intelligence Service), or the Federal Ministry of Defence (for the Military Counterintelligence Service). The corresponding orders may only concern persons against whom there are factual indications of vigorously promoting the severe threats meant to be cleared up with

---

[4] *Bergemann*, in: Denninger/Rachor, Handbuch des Polizeirechts, p. 942.

the information request (Section 8a Subsection 3 No. 1 BVerfSchG), or concerning whom such indications do not exist, but where specific facts give rise to the assumption that they are using services for the benefit of such persons (Section 8a Subsection 3 No. 2a BVerfSchG). Originally, the Counter-Terrorism Act's period of validity was set to end in 2007. This period was first extended until 2016 and more recently again until 2021.[5]

d) Customs Investigation Service

Finally, Section 23a Subsection 1 of the Customs Investigation Act grants the Customs Investigation Office power to intercept telecommunication if facts support the assumption that persons are preparing certain offences specified in the War Weapons Control Act. According to Section 23a Subsection 3 of the Customs Investigation Act, such authorisation is also granted when facts support the assumption that persons are preparing the unlawful export of nuclear goods or certain goods designated for military deployment. The interception must be authorised by a judge.

3. Responsibility for the technical implementation of interception measures

The interception is carried out by the competent authority itself. The telecommunication service providers are only required to enable the authorities to perform their measure; compare, for instance, Section 100a Subsection 4 StPO, Section 2 Subsection 1 G 10. To this end, they are required to provide the authority with a copy of the extracted telecommunication, see Section 7 Subsection 1 of the Telecommunication Interception Regulation (*Telekommunikationsüberwachungsverordnung*, TKÜV). Knowledge of the communication's content is gained and recorded solely by the authority's employees, not by the telecommunication service provider's personnel. From a technical point of view, the surveillance is implemented by the respective *Länders'* Criminal Police Offices *(Landeskriminalämter)*, the Federal Criminal Police Office, the Customs Investigation Service, the Federal and State Offices for the Protection of the Constitution, the Military Counterintelligence Service, or the Federal Intelligence Service.

4. Legitimacy of data transfers between security agencies

The activities of prosecution authorities, of preventive police authorities, and of intelligence agencies are in principle segregated. Organisational overlaps occur only insofar as investigative measures of criminal procedure are regularly executed by the police authorities (which also perform preventive tasks). Under certain statu-

---

[5] Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen, BGBl. 2015 I p. 2161.

torily defined conditions, the disclosure to other authorities of data collected during such telecommunication interception measures is admissible. However, such a rededication requires a statutory authorisation, as personal data may in principle only be used for the (exact) purpose that justified their collection. Through this principle of purpose limitation, a proportionate balance is ensured between the investigative measure leading to the collection of the data on the one hand, and the purpose of the collected data's use on the other hand.[6]

a) Exchange of data between prosecution authorities and preventive police authorities

Rededicating data that was collected within the criminal procedure framework by way of telecommunication interception for the purpose of averting danger is possible in principle, see Section 481 Subsection 1 StPO and, e.g., Article 54 Subsection 2 BayPAG. If the data had been collected under the criminal procedure law through particularly intrusive measures (in particular the interception of telecommunication), *Länder* law sometimes specifies that such a rededication is admissible only for the purpose of averting a danger to life, health, or liberty of a person or for fighting certain serious crimes, see, e.g., Section 38 Subsection 1 Sentence 3 BWPolG.

In contrast, the possibilities for rededicating data collected during a preventively based measure of telecommunication interception for the purpose of criminal prosecution are more limited. Such data may only be used as evidence for the prosecution of crimes to the extent that the interception measure could also have been ordered pursuant to the Code of Criminal Procedure, see Section 161 Subsection 2 Sentence 1.

b) Disclosure of data by intelligence agencies

Under certain restrictive conditions, data gathered through the interception of telecommunication may be exchanged between intelligence agencies on the one hand, and police and prosecution authorities on the other hand. The disclosure of data collected by the intelligence authorities by way of telecommunication interception to police and prosecution authorities is only admissible if this is necessary for the prevention or prosecution of certain crimes related to state security, as well as certain other serious crimes, see Section 4 Subsection 4 in connection with Section 3 Subsection 1, 1a or Section 7 Subsection 4 G 10 for the telecommunication

---

[6] See BVerfG NJW 1984, 419; *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, BDSG 2003 Section 13, para. 2; *Petri*, in: Denninger/Rachor, Handbuch des Polizeirechts, p. 839.

interception in individual cases, and Section 7 Subsection 4, Section 8 Subsection 6 G 10 for the strategical interception of telecommunication.

c) Disclosure of data to intelligence agencies

The disclosure of data collected by prosecution authorities during telecommunication interception measures to intelligence agencies is also only permissible to a limited extent. The disclosure to the Federal Office for the Protection of the Constitution, the Federal Intelligence Service, or the Military Counterintelligence Service is admissible only if there exists suspicion of the commission of certain offences pertaining to state security, see Section 18 Subsection 6, Section 22 BVerfSchG, and Section 23 Subsection 4 BNDG. Similarly, the disclosure of data gathered during preventive telecommunication interception by the *Länder's* police authorities is restricted in the *Länder's* police laws, and usually does not, or only under narrow conditions, permit a disclosure to intelligence agencies.[7]

B. Statistics on Telecommunication Interception

1. Obligation to collect statistics

In the field of criminal prosecution, a legal obligation to compile detailed statistics concerning the number of telecommunication interception measures exists with regard to measures carried out under Sections 100a StPO (telecommunication interception), 100b StPO (online search) and 100g StPO (telecommunications connection data and radio cells data requests). As stipulated in Section 101b StPO, the *Länder* and the Attorney General report annually to the Federal Office of Justice *(Bundesamt für Justiz)* on the telecommunication interception measures ordered within their respective area of competence. The Federal Office of Justice then prepares a summary of the measures ordered nationwide during the reporting year and publishes it on the internet.

In this respect, Section 101b Subsection 2 StPO requires the disclosure of the number of proceedings in which telecommunication interception was ordered, the number of interception orders issued (differentiating between initial and extension orders), the underlying offences prompting the respective measures, and the number of proceedings in which, for the purpose of enabling the interception, access to the communication participant's terminal device was ordered and effectively carried out. Section 101b Subsection 3 StPO furthermore requires the disclosure of the number of proceedings in which an online searche was ordered, the number of

---

[7] See Article 48 Subsection 2 and Article 56 Subsection 2 BayPAG; see also *Petri*, in: Denninger/Rachor, Handbuch des Polizeirechts, pp. 867 et seq.

online search orders issued (differentiating between initial and extension orders), the underlying offences prompting the measure, and the number of proceedings in which the communication participant's terminal device was effectively accessed. Finally, section 101b Subsection 5 StPO requires disclosure of the number of proceedings in which requests for communications data or radio cells data have been ordered, the number of initial and extension orders, for each case the number of weeks covered by the order, the number of orders that, due to a lack of the requested data, were partially inconclusive, and the number of orders that, due to a lack of the requested data, were fully inconclusive.

Pursuant to Section 1 Subsection 1 of the Act on the Parliamentary Control of Federal Intelligence Activities (*Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes*, PKGrG), the measures executed within the framework of the Counter-Terrorism Act (i.e., the gathering of customer and user-related information from telecommunications and teleservice providers, and the use of IMSI-catchers) are subject to the control of the Parliamentary Control Panel. The Panel annually provides the *Bundestag* with a report on the implementation, type, scope, and the grounds for ordering such measures, stipulated in Section 8b Subsection 3 Sentence 2 and Subsection 10 Sentence 1, Section 9 Subsection 4 Sentence 7 BVerfSchG, Section 3 Subsection 1 Sentence 3, Section 5 Sentence 2 BNDG and Section 4a Sentence 1, Section 5 MADG.

2. Current data

a) Law enforcement authorities

aa) Measures pursuant to Section 100a StPO

The Federal Office of Justice's statistics on the number of measures ordered by the *Länder* and the Attorney General pursuant to Section 100a StPO hardly changed between 2011 and 2014.[8] However, the number of orders for the interception of internet communication increased between 2011 and 2016.

Orders pursuant to § 100a StPO (Germany as a whole)						
Year	**Procedures**	**Number of interception orders issued**		**Type of communication intercepted**		
		Initial orders	Extension orders	Landline	Mobile	Internet
2011	5516	18,029	3089	3621	17,568	1345
2012	5678	19,616	3445	3902	19,666	4476

[8] Find the annual statistics at https://www.bundesjustizamt.de/DE/Themen/Buerger dienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html

2013	5669	19,398	3519	3271	19,670	5033
2014	5625	19,795	3587	3303	20,499	5485
2015	5945	18,640	3950	3332	21,905	7431
2016	5738	17,510	3845	3856	21,236	10,606
2017	5629	15,669	2982	3606	20,022	9508

bb) Measures pursuant to Section 100g StPO

Over recent years, the Federal Office of Justice's statistics on the measures ordered pursuant to Section 100g StPO have shown a marked rise both in the total number of proceedings as well as in the number of initial orders issued.

Year	Procedures	Number of interception orders issued	
		Initial orders	Extension orders
2011	7986	13,743	410
2012	9901	17,137	462
2013	12,572	20,242	681
2014	13,979	21,926	775
2015	16,117	26,265	899
2016	16,363	25,640	864
2017	15,361	22,929	711

b) Intelligence agencies

The law requires the federal Parliamentary Control Panel to provide details about the scope of telecommunications surveillance,[9] requests of customer and user-related information from telecommunication and teleservices providers and the use of IMSI-catchers by the federal intelligence services.[10]

---

[9] Parliamentary Control Panel report of 24 May 2019 in BT-Drs. 19/10459, pp. 5, 8, 9. In the year 2017, altogether 276 targeted interception measures were authorized for the BfV, the BND and the MAD, thereof 235 concerned the BfV and 34 the BND. As regards strategic interception by the BND, the report specifies that in 2017, 13,829 search terms were authorized and, on this basis, 119 telecommunication connections identified as relevant.

[10] For requests to telecommunication and teleservice provider and the use of IMSI-catchers, see the Parliamentary Control Panel's report of 24 May 2019 in BT-Drs. 19/10460.

aa) Request for information from telecommunication and teleservice companies

The following statistics cover requests for information under Section 8a Subsection 2 Nos. 4 and 5 BVerfSchG, Section 3 Subsection 1 BNDG and Section 4a MADG concerning traffic data pursuant to Section 96 Subsection 1 Nos. 1 to 4 of the Telecommunication Act (*Telekommunikationsgesetz*, TKG), as well as corresponding data collected by teleservices. In 2017, as in the years before, the majority of requests for information served the purpose of investigating Islamist activities.[11]

Year	BfV	BND	MAD
2010	42	0	1
2011	34	0	0
2012	34	0	0
2013	54	0	0
2014	37	0	2
2015	38	0	0
2016	67	0	0
2017	46	0	0

bb) IMSI-Catcher

The same holds true for the use of IMSI-catchers pursuant to Section 9 Subsection 4 Sentence 1 BVerfSchG, Section 5 Sentence 2 BNDG and Section 5 MADG: Their employment, executed exclusively by the Federal Office for the Protection of the Constitution, in 2017 again primarily targeted Islamist activities.[12]

Year	IMSI-catcher-deployment by the BfV
2010	16
2011	14
2012	17
2013	26
2014	16
2015	18
2016	18
2017	28

[11] Parliamentary Control Panel report of 24 May 2019, BT-Drs. 19/10460, p. 8.

[12] *Ibid.*, p. 9.

II. Principles of Telecommunication Interception in Constitutional and Criminal Procedural Law

A. Constitutional Safeguards of Telecommunication

1. Areas of constitutional protection

a) Secrecy of telecommunication

Article 10 of the German Basic Law (*Grundgesetz*, GG) represents the central constitutional norm safeguarding the secrecy of telecommunication. It protects the confidentiality of the incorporeal transmission of information to an individual recipient using telecommunication devices. The secrecy of telecommunication covers both the content of telecommunication as well as the circumstances of the communication process. Thus, telecommunications traffic data are protected from state knowledge and from being processed.[13] Data subsequently stored in the communication service provider's sphere continue to be protected by the secrecy of telecommunication even when the communication's content has already reached its recipient.[14]

b) Confidentiality and integrity of information systems

Data stored on a computer are afforded protection by the fundamental right to confidentiality and integrity of information systems, a construction by the Federal Constitutional Court *(Bundesverfassungsgericht)*. It primarily offers protection against secret access to an information system, by way of which the system's use could be monitored and its storage media surreptitiously read.[15]

c) Core area of privacy

Furthermore, the interception of telecommunication must respect an inviolable area of privacy, the protection of which follows from the constitutional primacy of human dignity. Each individual must have the opportunity to express him- or herself without fear of being monitored by government institutions: this includes things such as sentiments and feelings, reflections, opinions, and experiences of a strictly personal nature. This core area of privacy is deemed absolutely inviolable. Even substantial public interests cannot justify an infringement.[16] However, only such investigative measures are precluded that render likely the capture of uncondi-

---

[13] BVerfG NJW 2006, 976 (978); NJW 2008, 822 (825); NJW 2010, 833 (835); NJOZ 2010, 1492 (1493).

[14] BVerfG NJW 2009, 2431.

[15] BVerfG NJW 2008, 822.

[16] BVerfG NJW 2004, 999 (1002); NJW 2012, 907 (908); NJW 2016, 1781, 1787.

tionally protected information. The obtainment of such communication content in other ways merely leads to the prohibition of its utilisation.[17] Thus, communication is protected when it takes place between persons sharing a special relationship of trust within the scope of this core area. This may concern family members or other very close friends. However, this protection is afforded only as long as there are no concrete indications that the conversation's expected content will exhibit an immediate connection to a criminal offence.[18]

d) Right to informational self-determination

Personal data are also protected by the constitutionally guaranteed right to informational self-determination. It gives individuals the right to decide in principle on the disclosure and use of their personal data. In particular, this protects the placement of reasonable faith in the identity of one's communication partner. Communication content stored in the recipient's sphere after conclusion of the communication process is covered solely by this fundamental right; it is no longer covered by the constitutional protection of the secrecy of telecommunication.[19] Furthermore, the right to informational self-determination provides protection against government bodies purposefully compiling, storing, and possibly analysing together with other data such information as was acquired by screening publicly available content in the absence of a statutory basis.[20] Due to their constituting an encroachment on the right to informational self-determination, such measures require a proportionate statutory basis justified by a prevailing general interest.[21] When assessing the gravity of the encroachment connected with an investigation measure, the processed data's relevance to personality is of special significance.[22] A measure is considered highly invasive in particular when the relevant data allow conclusions about the nature and intensity of interpersonal relationships, personal interests, habits and tendencies, or the content of communication.[23]

---

[17] See BVerfG NJW 2012, 907 (908).

[18] BVerfG NJW 2004, 999 (1003), NJW 2008, 822 (833); NJW 2016, 1781, 1787.

[19] BVerfG NJW 2006, 976 (978); BVerfG NJW 2008, 822 (825); NJW 2009, 2431 (2432).

[20] BVerfG NJW 2008, 822 (836). For more on so-called internet investigations, see *Böckenförde*, JZ 2008, 925 (935).

[21] See BVerfG NJW 1984, 419; *Di Fabio*, in: Maunz/Dürig, Grundgesetz-Kommentar, Article 2, paras. 179 et seq.

[22] BVerfG NJW 2007, 2464 (2470).

[23] See BVerfG NJW 2006, 976 (980).

2. Proportionality of access to data

The Constitution demands that all forms of government intervention in an individual's rights be proportionate. The principle of proportionality requires that every encroachment on fundamental rights serve a legitimate purpose, be suitable for achieving its objective, and be necessary and proportionate to the objective pursued.[24]

a) Implications for encroachments on the secrecy of telecommunication

The invasion of privacy, coupled with the secrecy employed in the process, give the interception of telecommunication a high degree of invasiveness.[25] With respect to the principle of proportionality, telecommunication interception thus belongs to the most demanding procedural investigative measures, as far as prerequisites are concerned.

b) Implications for access to traffic data

The principle of proportionality is also of relevance for the access to telecommunication traffic data. In line with decisions by the Federal Constitutional Court, the invasiveness of such measures is rising due to the continuing digitalisation of telecommunication. The quantity and the substance of accruing traffic data serve to paint an ever clearer picture of communication participants. Increasingly, communication data allow conclusions to be drawn about their personality, and even the generation of a personality profile becomes a real possibility.[26] Considering this, the access to mere traffic data (without even targeting communication content) is in and of itself viewed as a significant encroachment on the secrecy of telecommunication.

c) Implications for intrusion into information systems

Finally, the principle of proportionality is also of particular importance for secret intrusions into information systems. Privately or commercially used computers or comparable terminal devices (such as mobile phones) may contain such vast and varied amounts of personal data that access to these systems can provide insight into a significant part of a person's private life. It may also enable a meaningful analysis of one's personality.[27] Clandestine access to an information system thus gives the acting government body access to a stock of data that easily surpasses what traditional sources of information can offer with respect to scope and variety.[28]

---

[24] BVerfG NJW 2007, 2464 (2468); NJW 2008, 822 (828).
[25] See BVerfG NJW 2008, 822 (830).
[26] BVerfG NJW 2006, 976 (980).
[27] BVerfG NJW 2008, 822 (827).
[28] BVerfG NJW 2008, 822 (829).

3. Consequences for the interception of telecommunication

a) Protection of the secrecy of telecommunication

In accordance with Article 10 Subsection 2 GG, an encroachment on the secrecy of telecommunication (encompassing both the access to communication content and traffic data) requires statutory authorisation. Considering, with a view to the principle of proportionality, the highly invasive character of accessing the content of ongoing telecommunication, considerable requirements must be met. In particular, the interception of telecommunication is admissible only for the prosecution of *serious* criminal offences.[29]

b) Protection of the confidentiality and integrity of information systems

The prosecution authorities' possibilities for secretly accessing terminal devices for interception purposes are limited by the fundamental right to confidentiality and integrity of information systems. Secret access to information systems (espionage of stored data or surveillance of system utilisation) is considerably more invasive than the interception of ongoing telecommunication. If a measure of telecommunication interception is not to be evaluated as an encroachment of this nature (but merely as an encroachment on the secrecy of telecommunication), then it must be technically ensured that data on the terminal device unrelated to the ongoing telecommunication are not accessed simultaneously.[30] However, the secret extraction of data not stemming from ongoing communication by clandestine access to a person's terminal device is – within narrow limits – constitutionally admissible., and it is now admissible for the investigation of a number of serious or very serious crimes (Section 100b StPO).[31] Furthermore, the Federal Criminal Police Office and the police of some *Länder* are now also authorised to secretly interfere with the integrity of information systems for adverting dangers to life, limb, freedom and dangers to goods that are of paramount importance for the Federation, a *Land* or the general public (Section 49 Subsection 1 BKAG; see also Article 45 Subsection 1 BayPAG; Section 15c HSOG).[32]

c) Protection of the core area of privacy

Further constitutional requirements for the interception of telecommunication also result from the constitutional protection of the core area of privacy. A communi-

---

[29] On the temporal scope of Article 10, see *Sieber/Brodowski*, in: Handbuch Multimedia-Recht, part 19.3 paras. 119–121.

[30] BVerfG NJW 2008, 822 (825 et seq.); NJW 2016, 1781, 1786.

[31] *Sieber/Brodowski*, in: Handbuch Multimedia-Recht, part 19.3 paras. 158–160.

[32] *Graf*, Beck-OK StPO, Section 100b, para. 4.

cation's relevance to this core area must be considered both before ordering an interception measure and during its performance. Depending on the conclusions of this consideration, the measure must be refrained from or collected data must be deleted, where necessary (see also below III.B.3.a.bb.).[33]

4. Statutory protection of personal data

a) Criminal liability for the unlawful infringement of telecommunication

The unlawful overhearing or recording of non-publicly spoken words is punishable in accordance with Section 201 of the German Criminal Code (*Strafgesetzbuch*, StGB). The violation of the secrecy of telecommunication by an employee of a telecommunication service provider can also entail a criminal sentence pursuant to Section 206 StGB. The unlawful obtaining of data especially protected against unauthorised access is punishable under Section 202a StGB when accomplished by circumventing such protection. Finally, the unauthorised obtaining of data by technical means from a non-public transfer of data is declared a criminal offence in Section 202b StGB.

b) Protection of professional secrets in criminal procedural law

Certain information worthy of protection is safeguarded by Section 160a in connection with Sections 53, 53a StPO against investigative measures of criminal procedure. This includes, in particular, communication within certain relationships of trust, such as with clergy, attorneys-at-law, and medical practitioners. Some of these statutory regulations protect the constitutional core area of privacy.

c) Principle of "purpose limitation of personal data"

The powers of criminal procedure are also shaped by the principle of purpose limitation of personal data. This principle declares that data may generally be used only in accordance with the purpose they were collected for. Subsequently, personal data obtained through investigative measures must be deleted when and to the extent that they are no longer required for the purpose they had been collected for. Among other things, Section 101 Subsection 8 StPO thus prescribes the mandatory deletion of data acquired through telecommunication interception once they are no longer necessary for criminal prosecution. As a consequence of the principle of purpose limitation, any amendment to the initial purpose of the collection requires a statutory basis. Section 477 Subsection 2 Sentence 2 StPO constitutes such a basis. According to this provision, if a measure is only admissible where specified criminal offences are suspected, then any personal data obtained on the basis of

---

[33] BVerfG NJW 2016, 1781 (1787); 2008, 822 (834); NJW 2016, 1781, 1787.

such a measure may be used for evidentiary purposes in other criminal proceedings only if they concern a criminal offence, for the prosecution of which such a measure could have been ordered.

B. Powers in the Code of Criminal Procedure

1. Requirement of (reasonable) clarity for powers in the law of criminal procedure

Powers in the law of criminal procedure must satisfy the constitutional requirements of clarity and specificity. They are to ensure that the democratically legitimised parliamentary legislature itself must make all substantial decisions on the infringement of fundamental rights and the scope of the encroachments. Clarity and specificity of a provision are also meant to enable citizens to inform themselves about the legal situation in advance and show them which encroaching measures they might have to expect. The legislature must therefore, in a sector-specific way, determine occasion, purpose, and limits of invasive actions with sufficient precision and legal clarity.[34] Infringements of lower intensity, however, may be justified on the basis of statutory general clauses.[35]

2. Differentiation and classification of powers in the law of criminal procedure

The Code of Criminal Procedure furnishes law enforcement authorities with a differentiated arsenal of coercive powers. As a rule, the more invasive a measure, the more precisely defined are the possible predicate offences, the necessary degree of suspicion, and the manner of a measure's implementation.

III. Authority to Access Telecommunication Data in the Law of Criminal Procedure

A. Overview

The secret interception of ongoing telecommunication is authorised by Section 100a StPO. Communication data saved on storage media can additionally be obtained by way of open seizure of the storage medium pursuant to Section 94 StPO and its surrender can be demanded in accordance with Section 95 StPO. As

---

[34] BVerfG NJW 2004, 2213 (2215); NJW 2008, 822 (827 et seq.).

[35] See BGH NJW 1991, 2651; *Pfeiffer*, Strafprozessordnung, Section 161, para. 1.

stipulated by Section 110 Subsection 3 StPO, during a search pursuant to Sections 102 et seqq. StPO, the examination of an electronic storage medium may be extended to cover physically separate storage media (such as a server accessible online), insofar as they are accessible from the storage medium. Finally, Section 100g StPO grants access to traffic data and Section 100j StPO grants access to subscriber data stored with the telecommunication service provider.

B. Interception of Content Data

1. Statutory empowerment

The main provision in the law of criminal procedure dealing with the interception of telecommunication is Section 100a Subsection 1 StPO. It reads as follows (excerpt only):

> (1) Telecommunication may be intercepted and recorded even without the knowledge of the persons concerned if
>
> 1. certain facts give rise to the suspicion that a person, either as perpetrator or participant, has committed a serious criminal offence referred to in Subsection 2 or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence; and
> 2. the offence is one of particular gravity in the individual case as well; and
> 3. other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success.

Section 100a Subsection 2 StPO lists the serious criminal offences that Subsection 1 makes reference to. An overview over these offences can be found in the annex to this report.

2. Scope of application

a) Object of interception

Section 100a StPO authorises prosecution authorities to intercept "telecommunication." This term, however, is not defined in the Code of Criminal Procedure. According to present case law, the term "telecommunication" describes the incorporeal transmission of information through electromagnetic or optical signals, similar to the interpretation in the Telecommunication Act.[36] But aside from that, a multitude of

---

[36] BVerfG, ZD 2017, 132 (132 et seqq.); BGH NStZ 2003, 668 (669); KK/*Bruns*, Section 100a, para. 4; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 6. However, the Federal Constitutional Court favours a more generous interpretation of "telecommunication" as used in Article 10 Subsection 1 GG: It does not support the "purely technical understanding of telecommunication found in the TKG," but chooses to focus instead "on the

questions concerning the provision's scope of application remain due to the lack of an explicit statutory clarification. These questions have yet to be answered fully by the courts.

aa) Content of communication

Apart from analogous communication between persons, Section 100a StPO also covers the internet-based and other electronic transmission of voice, symbols, pictures, and sound. Not only are telephone and email captured, but also chats, messaging, online fora, and other confidential communication.[37] The specific mode of transmission used (cable-bound or wireless, analogous or digital) is irrelevant.[38] The term "telecommunication" also covers data which do not form the actual content of the message: in particular, this applies to the transmission of traffic data between a communication service provider and the terminal devices of the communication participant.[39]

bb) Communication between persons

A prerequisite for the interception of telecommunication pursuant to Section 100a StPO is that a person uses telecommunication equipment, meaning he or she communicates by means of such equipment.[40] The automated, and consequently non-deliberate, reception of messages on an answering machine, or the arrival of email in a mailbox, and even the unsuccessful attempt at establishing a communication connection also all constitute telecommunication.[41]

According to the (controversial) opinion of the first chamber of the second senate of the Federal Constitutional Court, when data transfer takes place exclusively between technical devices, it only constitutes telecommunication if these data (concerning, e.g., the data exchange between a mobile device and the mobile provider during a conversation) accrue in connection with a specific telecommunication process or while establishing a telecommunication connection. Telecommunication thus requires an individualised exchange of information induced by a human being.[42] Consequently, such data that a mobile device transmits to the network in standby mode in order to show its operative readiness would not constitute tele-

---

holder of the fundamental right and his need for protection due to the involvement of third parties in the process of communication," BVerfG NJW 2009, 2431 (2433).

[37] KK/*Bruns*, Section 100a, paras. 20 and 23; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, paras. 6–6c; *Singelnstein*, NStZ 2012, 593 (595).

[38] BVerfG NJW 2007, 351 (353); NJW 2009, 2431 (2432).

[39] BGH NStZ 2003, 668 (669).

[40] *Ibid*.

[41] *Ibid*.

[42] BVerfG NJW 2007, 351 (353).

communication.[43] Nevertheless, it is unclear to what extent this decision can be applied to IP data transfers[44] or to automated data transfers that reveal more sensitive information about the user of a technical device.[45]

cc) Surfing as telecommunication

In line with this broad construction of "telecommunication," Section 100a StPO in principle covers all traffic of data with the internet by means of a telecommunication device. Thus, the upload and download of data to or from third party servers is also captured.[46] Some parts of the literature and the third senate of the Federal Constitutional Court assume that the surveillance of such data flows is unconditionally permissible.[47] Some academic literature is however of the opinion that at least the surveillance of surfing behaviour during the capture of IP-based data transfers is not covered by the term "telecommunication" as used in the Code of Criminal Procedure.[48]

b) Temporal limits of telecommunication

aa) Access to ongoing telecommunication

According to the courts, the interception of telecommunication covers the technological process of sending, transmitting, and receiving messages.[49] The drafting of a message for later transmission and the connected storage of this draft therefore does not represent a part of the communication process.[50] Despite much criticism in academic literature[51] accessing the content of messages during ongoing communication even while the data are still on the sender's system, i.e., had not left it yet, with the aim of sidestepping encryption was, in the past, deemed per-

---

[43] BVerfG NJW 2007, 351 (353).

[44] *von zur Mühlen*, Zugriffe auf elektronische Kommunikation, pp. 121 et seqq.

[45] *Sieber/Brodowski*, in: Handbuch Multimedia-Recht, part 19.3 para. 134.

[46] BVerfG NJW 2016, 3508, 3509, 3510; also *Kudlich*, GA 2011, 193 (199); *Sieber/Brodowski*, in: Handbuch Multimedia-Recht, part 19.3 para. 133.

[47] BVerfG, ZD 2017, 132 (132 et seqq.); see also LG Ellwangen, decision of 28 May 2013 – 1 Qs 130/12; critical of the decision *Albrecht/Braun*, HRRS 2013, 500 et seqq. For a broader analysis of this issue see *von zur Mühlen*, Zugriffe auf elektronische Kommunikation, pp. 257 et seqq.

[48] *Hiéramente*, StraFo 2013, 96 et seq.; *Albrecht/Braun*, HRRS 2013, 500 et seq.; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 7b.

[49] BGH NStZ 2003, 668 (669); KK/*Bruns*, Section 100a, para. 18.

[50] *Kudlich*, GA 2011, 193 (202).

[51] *Becker/Meinecke*, StV 2011, 50 (52); *Braun*, jurisPR-ITR 3/2011; *Brodowski*, JR 2011, 533 (537); *Buermeyer/Bäcker*, HRRS 2009, 433 (439); *Kudlich*, GA 2011, 193 (206); *Sieber*, Gutachten 69. Deutscher Juristentag, C 104 et seq.; *Wolter*, in: SK-StPO, Section 100a, para. 27.

missible by some practitioners.[52] However, insofar as encroachments on the integrity of the sender's information system are now explicitly allowed by law for this purpose, the question is now considerably less relevant (for more on the relevant issues as well as further aspects of so-called source telecommunication surveillance, see below III.B.2.c.aa.).[53]

bb) Access after the end of telecommunication transmission

Access to communication data already received and stored in the exclusive sphere of the recipient (on the hard drive or mobile phone, for instance) is not covered by telecommunication interception.[54] The same holds true for data stored in the exclusive sphere of the sender. However, emails stored with the recipient's mail provider can be classified as belonging to the transmission process even after they are retrieved by their recipient. In this respect, the courts allow accessing the data stored by the mail provider in accordance with the regulations on seizure: in contrast to telecommunication interception, this measure must be performed overtly.[55] Nonetheless, covertly accessing the emails stored by the mail provider still remains possible on the basis of Section 100a StPO, precisely because the communication process is deemed to be continuing in the form of email storage by the mail provider – even after their retrieval by the recipient (for more, see D.2.c.bb.(2)).[56]

Although the issue has not been explicitly resolved in law, this also means that Section 100a StPO is applicable when confidential communication (such as in social networks or private chatrooms) is exchanged on a communication platform simultaneously viewed by all communication participants and real time access to this communication ensues secretly.[57] For non-real time access on such communication platforms, the deliberations concerning access to emails apply accordingly.[58]

---

[52] LG Landshut NStZ 2011, 479; LG Hamburg MMR 2011, 693.

[53] LG Landshut NStZ 2011, 479; LG Hamburg MMR 2011, 693; KK/*Bruns*, Section 100a, paras. 42–44; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 7a; in contrast, however, see LG Hamburg MMR 2008, 423.

[54] BVerfG NJW 2006, 976 (978); NJW 2009, 2431 (2432); KK/*Bruns*, Section 100a, para. 5.

[55] BGH NStZ 2009, 397 (398); KK/*Bruns*, Section 100a, para. 20.

[56] BVerfG NJW 2009, 2431 (2434); BGH NJW 2010, 1297 (1298).

[57] KK/*Bruns*, Section 100a, para. 23; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 7; *Singelnstein*, NStZ 2012, 593 (597); of a different view *Meinicke*, StV 2012, 463 (464).

[58] KK/*Bruns*, Section 100a, para. 23; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 6c; Section 100a, para. 6c.

c) Current matters of dispute

Some of the issues not yet conclusively resolved by the courts concerning Section 100a StPO's scope of application are particularly contentious.

aa) Source telecommunication surveillance

Before the issue has recently been addressed by legislation, some academic literature demanded that – contrary to prior practice, as approved of by courts of lower instance[59] – source telecommunication surveillance could not have been based on the power to intercept telecommunication.[60] They claimed that source telecommunication surveillance required an independent statutory authorisation as it encroaches on the integrity of the targeted information system and this invasion of the communication partner's information system creates the possibility of accessing extensive amounts of data, above and beyond the individual communication. Even assuming such access were non-deliberate, the mere risk of data being obtained without authorisation leads to a significant increase in the measure's invasiveness. Source telecommunication surveillance thus impacts not only the constitutionally protected secrecy of telecommunication because of the connected secret invasion of information systems, but also concerns the constitutional right of personality in the form of a right to integrity and confidentiality of information systems. In consequence, its prerequisites are more rigorous than for the mere interception of telecommunication. The Federal Constitutional Court views source telecommunication surveillance as encroaching only upon the secrecy of telecommunication provided it is ensured that the surveillance is limited exclusively to data from ongoing telecommunication, in other words when no data outside of the ongoing telecommunication are obtained while accessing the communication participant's terminal device. This, however, must be ensured by technical means and legal standards.[61] Academic literature sometimes questions whether it is technically feasible to comply with the Federal Constitutional Court's demand for a limitation to data from the ongoing communication process.[62] Despite such concerns, and as a result of the constitutional jurisprudence, separate legal provisions governing source telecommunication surveillance were introduced. Federal legislation and some *Länder* police laws now provide special requirements to ensure that source telecommunica-

---

[59] LG Landshut NStZ 2011, 479; LG Hamburg MMR 2011, 693.

[60] *Braun*, jurisPR-ITR 3/2011; *Brodowski*, JR 2011, 533 (537); *Buermeyer*/*Bäcker*, HRRS 2009, 433 (439); *Sieber*, Gutachten 69. Deutscher Juristentag, C 104 et seq.; *Wolter*, in: SK-StPO, Section 100a, para. 27.

[61] See BVerfG NJW 2008, 822 (826); NJW 2016, 1781, 1796.

[62] *Buermeyer/Bäcker*, HRRS 2009, 433 (439); *Singelnstein*, NStZ 2012, 593 (598); *Sieber/Brodowski*, in: Handbuch Multimedia-Recht, part 19.3 para. 150; see also *Müller*, NZWiSt 2020, 96 (98).

tions surveillance complies with the conditions set by the Constitutional Court.[63] Section 100a para. 1 StPO now explicitly provides that "[t]elecommunications may also be intercepted and recorded in such a manner that technical means are used to interfere with the information technology systems used by the person concerned if this is necessary to enable interception and recording in unencrypted form in particular." In addition, the reformed provision allows for the interception of the "content and the circumstances of the communication stored in the person concerned's information technology systems" even after the the communication, provided that this information "could also have been intercepted and recorded in encrypted form during ongoing transmission processes." Insofar as this seems to go beyond an interception of telecommunications and instead signifies the power to covertly access a person's information system, the constitutionality of this provision is now subject to debate.[64]

bb) Accessing external storage media as communication

Not yet decided by the superior courts is whether or not such data transfers are to be treated as telecommunication which are caused by someone accessing external storage media over the internet – as is the case with cloud computing – in order to retrieve their own data, thus not constituting communication from another person.[65] In light of the courts' interpretation of "telecommunication" outlined above, in principle it seems permissible to intercept the respective up- and downloads from or to the internet user's terminal device on the basis of Section 100a StPO.[66] Some academics, however, demand that the exchange of data between the internet user and their online-accessible external storage media not be treated as telecommunication.[67] Particularly when considering the outsourcing of data from a stationary hard drive to a cloud provider's server, they say it becomes clear that accessing such a transfer of data is – contrary to a formal view (data transfer between the operator of an external server and the internet user) – functionally not an equivalent to accessing communication between persons. Instead, it equates to a secret search of an internet user's internal store of data. Such an encroachment is therefore much more invasive than the interception of telecommunication with another per-

---

[63] See, e.g., Section 100a Subsection 1 s. 2, Subsection 5 StPO; Article 42 Subsection 2 BayPAG; Section 10c HamDVPolG; Section 15b HSOG; *Klesczewski*, ZStW 123 (2011), 737 (744); *Sieber*, Gutachten 69. Deutscher Juristentag, C 105; *Wolter*, in: SK-StPO, Section 100a, para. 30.

[64] *Sieber/Brodowski*, in: Handbuch Multimedia-Recht, part 19.3 para. 151.

[65] For it *Singelnstein*, NStZ 2012, 593 (595); against it *Sieber*, Gutachten 69. Deutscher Juristentag, C 107. For a detailed analysis see *von zur Mühlen*, Zugriffe auf elektronische Kommunikation, pp. 257 et seqq.

[66] BVerfG, ZD 2017, 132 (132 et seqq.); *Kudlich*, GA 2011, 193 (207).

[67] *Braun*, jurisPR-ITR 18/2013.

son. It rather resembles an online search and thus, in the opinion of these academics, should not be treated as the interception of telecommunication.[68] Insofar as such data is in practice captured as part of telecommunications interceptions, the data must therefore not be used, except in cases that satisfy the more demanding legal requirements of a remote online search.[69]

cc) Evaluation of surfing behaviour

The application of Section 100a StPO to the documentation and analysis of an internet user's surfing behaviour is controversial, but has been considered as permissible by the third senate of the Federal Constitutional Court assume that the surveillance of such data flows is unconditionally permissible.[70] To be sure, publicly accessible websites do not represent confidential information.[71] The question to what extent accessing websites constitutes telecommunication within the meaning of Section 100a StPO is, despite the recent constitutional jurisprudence, however not conclusively resolved yet. The analysis of surfing behaviour and particularly of queries on search engines often facilitates extensive conclusions about the user's personality and may even allow for the creation of a comprehensive character profile. Some therefore claim the invasiveness of surfing behaviour analysis to be much greater than that of intercepting interpersonal communication, leading some academics to oppose a corresponding application of Section 100a StPO under these circumstances.[72]

3. Special protection of confidential communication content

For certain kinds of communication content, the Code of Criminal Procedure provides special protection against investigative measures. Moreover, the courts have derived additional safeguards from the Constitution. The privileging of certain information affects the implementation of interception measures, and may also have an impact upon the obtained information's admissibility as evidence.

---

[68] *Sieber*, Gutachten 69. Deutscher Juristentag, C 107; *Singelnstein*, NStZ 2012, 593 (595).

[69] *Sieber/Brodowski*, in: Handbuch Multimedia-Recht, part 19.3 para. 133; on these requirements see below under III.D.

[70] BVerfG, ZD 2017, 132 (132 et seqq.); see also LG Ellwangen jurisPR-ITR 18/2013; against it *Braun*, jurisPR-ITR 18/2013.

[71] BVerfG NJW 2007, 351 (353); *Kudlich*, GA 2011, 193 (198).

[72] *Braun*, jurisPR-ITR 18/2013; *Albrecht/Braun*, HRRS 2013, 500 (504 et seq.); *Hiéramente*, StraFo 2013, 96 (100); *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 7b.

a) Privileged communication

aa) Professional secrets

(1) Unconditionally protected professional secrets

Section 160a Subsection 1 Sentence 1 in connection with Section 53 StPO affords unconditional protection against telecommunication interception to clergymen in their capacity as spiritual advisors, defence counsels of the suspect, attorneys, as well as members of the *Bundestag*, a *Landtag* (state parliament), or the European Parliament concerning information entrusted to them or that became known to them in this capacity. Also protected under Section 160a Subsection 3 in connection with Section 53a StPO are their assistants and persons involved in the professional activities as part of their training.

Interception measures which target persons entrusted with unconditionally protected professional secrets and which are likely to result in insights regarding the unconditionally protected information are prohibited pursuant to Section 160a Subsection 1 StPO. Information obtained in spite of this may not be used, not even as a mere clue in investigative proceedings.[73] Records thereof are to be deleted without delay. The circumstances of their obtainment and deletion, however, are to be documented. The same applies when, in the course of an investigative measure targeting someone not covered by this unconditional protection, information is obtained from the person and the obtained information itself is unconditionally protected.

If it becomes clear that one of the interlocutors is a defence counsel of the suspect, the interception must be aborted; should this be technically unfeasible, there must at least be no analysis of the conversation.[74]

(2) Conditionally protected professional secrets

Section 160a Subsection 2 in connection with Section 53 StPO affords conditional protection against telecommunication interception to patent attorneys, notaries, certified public accountants, sworn auditors, tax consultants, doctors, psychotherapists, pharmacists, midwives, members of a pregnancy counselling agency, and drug dependency counsellors in a counselling agency, concerning information entrusted to them or that became known to them in this capacity. Also protected under Section 160a Subsection 3 in connection with Section 53a StPO are their assistants and persons involved in the professional activities as part of their training.

Conditional protection is also granted to professional journalists as well as their assistants and persons involved in the professional activities as part of their train-

---

[73] *Schmitt*, in: Meyer-Goßner/Schmitt, Section 160a, para. 4.

[74] BGH StraFo 2005, 296; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 21.

ing. Protected subject matter includes information pertaining to origin and content of contributions, documents, and messages, and to profession-related perceptions. However, this applies only to the extent to which the materials concern the editorial part of the medium.

For cases in which the interception measure concerns a conditionally protected person and is likely to yield conditionally protected information, Section 160a Subsection 2 StPO determines that this circumstance is to be given special consideration when assessing a measure's proportionality. In procedures not concerning a criminal offence of substantial significance, the interest in criminal prosecution does not usually prevail. The measure must then be refrained from or, if this is an option for the kind of measure in question, be limited. This special principle of proportionality accordingly applies to the use of findings for evidentiary purposes. A criminal offence of substantial significance can be assumed when the specific offence exhibits at least an intermediate level of criminality, significantly disturbs peace under the law, or may significantly compromise the population's sense of legal security.[75] These prerequisites are usually not met when the offence is punishable by a maximum prison sentence of less than five years.[76] With criminal offences of substantial significance, the legitimacy of an interception measure or the exploitation of information gained through it depend upon a balancing of interests. Decisive factors include the interest in effective criminal prosecution and the reaching of a just decision on the one hand, and the public interest in the holder of the professional secret following his occupation as well as the individual's interest in not revealing the secret entrusted to him or her, on the other hand.[77]

(3) No protection in case of suspicion against the holder of professional secrets

In line with Section 160a Subsection 4 StPO, the provisions on unconditional and conditional protection of professional secrets are not applicable when factual indications give rise to the suspicion that the protected person is involved with the offence being investigated, or participated in giving aid to the offender after the crime, in obstructing justice, or in dealing with stolen goods. Concerning the suspect's defence counsel, however, the suspicion of having given aid, obstructed justice, or dealt with stolen goods for the benefit of the suspect is insufficient for precluding the proscription of interception.[78]

---

[75] See BVerfG NJW 2004, 999 (1010); NJW 2005, 1338 (1339).

[76] See BVerfG NJW 2009 2431 (2435).

[77] KK/*Griesbaum*, Section 160a, para. 14; *Schmitt*, in: Meyer-Goßner/Schmitt, Section 160a, para. 9a.

[78] *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 21.

bb) Protection of the core area of privacy

Special protection against telecommunication interception is accorded by Section 100d StPO to information pertaining to the core area of privacy.[79] This includes, for instance, the expression of innermost feelings or expressions of sexuality.[80] Protection of this core area can be assumed particularly when the person concerned communicates with people with whom he has a special relationship of trust connected with the core area. Such people may include close family members, priests, telephone pastors, criminal defence attorneys, or – in individual cases – doctors.[81] However, this does not apply when there are concrete indications that the content of the prospective conversation will have an immediate connection to the crime.[82]

When factual indications support the assumption that telecommunication interception would yield information exclusively from the core area of privacy, Section 100d Subsection 1 StPO declares the measure to be completely inadmissible. When such a relationship of trust becomes discernible, telecommunication interception may not be performed.[83] However, cases where measures can be expected to yield *exclusively* information from the core area will hardly ever occur in practice.[84] Thus, the Federal Constitutional Court considers it practically unavoidable in many cases that the investigative authorities will take notice of information during the telecommunication interception before they are able to recognise its connection to the core area; in these cases, the Constitution does not require refraining from the intrusion from the outset merely due to the risk of infringing the core area of privacy during the collection process.[85]

Apart from that, information from the core area of privacy obtained through the interception of telecommunication may not be utilised; Section 100d Subsection 2 StPO. Any recordings thereof are to be deleted without delay. The circumstance of their obtainment and deletion, however, are to be documented. The passing on or other use of content connected with the core area, even as investigative clues, is prohibited.[86]

---

79 BVerfG NJW 2005, 2603 (2611).

80 BVerfG NJW 2004, 999 (1003); NJW 2012, 907 (908).

81 BVerfG NJW 2012, 833 (837).

82 BVerfG NJW 2004, 999 (1003).

83 BVerfG NJW 2012, 833 (837).

84 This is reflected in the legislative reasons, which give communication with telephone counselling services offered by religious institutions as the sole example, see BR-Drs. 275/07, p. 98.

85 BVerfG NJW 2012, 833 (837).

86 BVerfG NJW 2012, 833 (838).

b) Responsibility for ensuring protection

The protection of professional secrets and the core area of privacy must already be considered by the public prosecution office when filing an application, as well as subsequently by the court charged with deciding on the application.

If, in exceptional circumstances, the continuation of an ongoing interception measure is noticeably and unquestionably inadmissible (this instance will be rare as interception is mostly performed by way of automated recording and not listened to in real time) then the investigators charged with performing the measure are required to discontinue the interception.[87]

After examining the data, the deletion of non-exploitable information is generally performed by the investigator who carried out the measure. The public prosecution office can be consulted before making a decision, provided this does not lead to an unwarranted delay to necessary deletion.[88] For other information, the public prosecution office decides on its usability in the course of the following proceedings.[89]

4. Performance of telecommunication interception

a) Performance by the authorities with or without the help of third parties

The interception of telecommunication can be performed by the telecommunication service provider extracting data and surrendering it to the prosecution authorities. This is the method generally used. Even when done in this way, only the prosecution authorities gain any knowledge of the communication's content.[90] Involving the telecommunication service provider is, however, not absolutely necessary. According to prevailing opinion, the prosecution authorities are also permitted to perform the interception by their own means,[91] for instance, by intercepting signals of a wireless network.[92]

b) Accompanying powers for the performance of interception

For telecommunication service providers, Section 100a Subsection 4 StPO stipulates a duty to cooperate in the technical execution of telecommunication interception. Furthermore, encroaching on the integrity of the targeted person's terminal

---

87 See BVerfG NJW 2012, 833 (838).

88 *Schmitt*, in: Meyer-Goßner/Schmitt, Section 160a, para. 5.

89 BVerfG NJW 2012, 833 (838).

90 BeckTKG-Komm/*Eckhardt*, Section 110, para. 31.

91 *Bär*, MMR 2008, 215 (219); *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 8; *Singelnstein*, NStZ 2012, 593 (599); of a different opinion *Wolter*, Section 100b, para. 19.

92 KK/*Bruns*, Section 100a, para. 5.

device is now explicitly allowed; Section 100a Subsection 1 Sentence 2 StPO.[93] Thereby, software is to be installed, which allows for circumventing the encryption of communication data by manipulating the processing of the data (so-called source telecommunication surveillance, see supra III.B.2.c.aa.). Section 100a Subsection 5 StPO specifies further requirements to ensure that an encroachment on the integrity of a terminal device does not lead to the monitoring or recording of information not directly related to an ongoing telecommunication. The legality of a physical intrusion into the concerned person's rooms as a preparatory measure based on Section 100a StPO is an issue of some controversy.[94]

5. Telecommunication service providers' duties to cooperate

In light of the regular necessity of having private communication service providers cooperate, their relevant duties have been extensively regulated.

a) Possible addressees of duties to cooperate

Pursuant to Section 100a Subsection 4 Sentence 1 StPO, all persons providing or contributing to telecommunication services are obliged to facilitate measures for the interception of telecommunication and to provide the required information without delay. The provision must be read in line with the terminology of the TKG: Pursuant to Section 3 No. 24 TKG, telecommunication services are services which consist completely or predominantly in the transmission of signals via telecommunication networks.[95] This includes access and network providers in particular, but also covers services that offer online communication as an internet application to the extent that the focus of their activities lies on the technical aspects of the telecommunication process.[96] Thus, email and VoIP services also fall under Section 3 No. 24 TKG, insofar as they provide an independent switching service.[97] Since Section 100a Subsection 4 Sentence 1 StPO also covers the *contribution* to the provision of telecommunications, the operators of the IT infrastructure are principally

---

[93] See KK/*Bruns*, Section 100a, para. 45; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 7a.

[94] BVerfG NJW 2008, 822 (826) apparently considers it legal; see also LG Hamburg MMR 2011, 693 (696).

[95] BeckTKG-Komm/*Eckhardt*, Section 110, para. 22; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 24.

[96] BeckTKG-Komm/*Eckhardt*, Section 110, para. 12; BerlKommTKG/*Säcker*, Section 3 paras. 72 et seq. Regarding the question of how application services on the higher internet protocol levels are covered by the TKG or the TMG (and regarding the proposal of a functional assessment for dealing with the issue), see *Brunst*, Anonymität im Internet, pp. 325 et seq., 380 et seq.

[97] If the providers simultaneously provide information of their own, this specific activity is subject to the TMG, cp. BerlKommTKG/*Säcker*, Section 3, para. 71.

also required to cooperate with the prosecution authorities. Furthermore, such access providers that do not themselves provide the identification in question, yet still temporarily contribute to the provision of an internet connection for this identification through roaming are also required to participate in interception measures.[98] Moreover, duties to cooperate and provide information pursuant to Section 100a Subsection 4 Sentence 1 StPO also exist for the operators of closed communication systems such as intra-company communication networks (e.g., in-house extensions and intranets).[99] This holds true regardless of whether telecommunication services are provided free of charge or in return for payment.[100]

b) Content of duties to cooperate

The interception order issued either by a court upon application of the public prosecution office or, in exigent circumstances, in the form of an order by the public prosecution office itself, entails pursuant to Section 100a Subsection 4 StPO that all persons providing or contributing to telecommunication services must enable the court, the public prosecution office, and officials working in the police force to implement measures pursuant to Section 100a Subsection 1 StPO and provide them with the required information without delay.

For operators of telecommunication facilities with which publicly available telecommunication services are rendered (for the entities this includes, see c.aa.), the technical and organisational implementation of the interception and the ensuing obligations are further specified in Section 110 TKG and in the TKÜV.[101] For telecommunication services not covered by the TKG and the TKÜV (i.e., in particular the operators of closed communication systems), these specific provisions do not apply.[102]

Pursuant to Section 5 Subsection 2 Sentence 1 TKÜV, the operator of a public telecommunication system must provide the authorised bodies (cp. Section 2 No. 3

---

98 BGH ErmR, NStZ 2003, 272.

99 KK/*Bruns*, Section 100a, para. 38; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 24.

100 Section 3 No. 24 TKG also views provision in exchange for payment as the norm, cp. BeckTKG-Komm/*Schütz*, Section 3, para. 78.

101 According to Section 110 Subsection 2 TKG, the Federal Government is empowered to make arrangements concerning the fundamental technical requirements and the key organisational aspects for the implementation of intercepts, and to determine the cases in which and the conditions under which compliance with certain technical requirements can be dispensed with on a temporary basis. The technical details are then stipulated by the Federal Network Agency pursuant to Section 110 Subsection 3 TKG. The permissibility of transmissions must, however, in all cases, still be determined based on the relevant specific regulation, i.e., Section 100a StPO in particular; regarding this, see BeckTKG-Komm/*Eckhardt*, Section 110, paras. 71, 72.

102 SK-StPO/*Wolter*, Section 100b, para. 24.

TKÜV) at the handover point with a full copy of the telecommunication taking place via its telecommunication system under the identification to be intercepted. For every intercepted identification, the authorised body supplies the obligated party with the designation of the recording lines to which the intercept copy is to be transferred.

According to Section 6 Subsection 1 TKÜV, the obligated party must ensure that these orders can be implemented without delay; the same applies for a premature abortion of the interception measure, if so required by the authorised body. Pursuant to Section 9 Subsection 1 TKÜV, the transmission principally is to take place via networks with switching functions.

Pursuant to Section 5 Subsection 1 No. 3 TKÜV, the duty to cooperate in the interception measure also covers telecommunication data contained in a storage facility allocated to the identification to be intercepted (such as a mobile identification or an email address). To this end, the telecommunication service providers must also facilitate accessing communication content routed directly to storage facilities allocated to the identification to be intercepted.[103] This concerns, e.g., voicemail stored in voicemail boxes, or messages stored on email servers. As part of the intercept copy, the telecommunication service provider must also provide the authorities with extensive traffic data concerning the intercepted telecommunication (such as the location of a mobile terminal device), see Section 7 Subsection 1 Sentence 1 TKÜV. This means that not only is the content of communication extracted, but also data regarding the specific circumstances of the communication.

c) Duties to provide technical and organisational infrastructure

aa) Obligated parties

Pursuant to Section 100a Subsection 4 Sentence 2 StPO in connection with Section 110 Subsection 1 Sentence 1 No. 1 TKG, the operators of telecommunication facilities that offer publicly available telecommunication services, must, at their own cost, maintain the technical means (hardware and software[104]) for the execution of telecommunication interception and make the organisational arrangements necessary for its prompt implementation. According to Section 110 Subsection 1 Sentence 1 No. 1a TKG, this maintenance duty also extends to forms of telecommunication that are based on the simultaneous utilisation of two or more telecommunication facilities (such as is particularly the case with VoIP telephony, where access providers and

---

[103] BMWi, reasoning behind the draft of a regulation on the technical and organisational implementation of telecommunication interception measures of 25 October 2001, p. 6 (available online at http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/20011025UllrichBegruendungTKUeV.pdf).

[104] BeckTKG-Komm/*Eckhardt*, Section 110, para. 30; BerlKommTKG/*Klesczewski*, Section 110, para. 34.

VoIP providers collaborate).[105] These provisions lead to telecommunication providers actively participating in the search for innovative solutions to ensure the ability to intercept VoIP telephony.[106] Pursuant to Section 110 Subsection 1 Sentence 2 TKG, persons that provide publicly available telecommunication services without operating the necessary telecommunication facility themselves must also assure that the operator of the facilities can implement telecommunication interception orders promptly. An obligation pursuant to Section 110 Subsection 1 TKG exists only when the services are offered within the TKG's scope of application. Thus, providers of publicly available telecommunication services using email servers located in a foreign country to provide email services in Germany are also covered.[107]

However, as per Section 3 Subsection 2 Sentence 1 TKÜV, these duties regularly do not apply to telecommunication services with less than 10,000 subscribers or other parties enjoying the right of use (No. 5), as well as network nodes for interconnection with the internet (No. 2). For the latter, there is an exception to the exception if they serve as switches between publicly available telephone services and international networks (so-called *Auslandsköpfe*; literally translated as "foreign heads"). Operators of closed communication systems are also not obliged to maintain a technical and organisational infrastructure, since they are not subject to Section 110 Subsection 1 Sentence 1 No. 1 TKG in the first place (see above).

bb) Individual technical obligations

The technical requirements for interception measures are defined in Sections 6 to 10 TKÜV. In particular, Section 7 TKÜV stipulates exactly which data are to be provided. According to Section 110 Subsection 3 TKG, the technical particulars concerning the implementation of telecommunication interception are stipulated in a detailed Technical Directive (TR TKÜV) by the Federal Network Agency *(Bundesnetzagentur)* with the participation of the associations of the telecommunication service provider industry, as well as the authorised bodies.[108] International technical standards are to be taken into consideration; deviations from the standards need to be justified with an explanation. In this way, one hopes to avoid standalone solutions and keep the costs for the parties involved as low as possible.[109]

---

[105] BeckTKG-Komm/*Eckhardt*, Section 110, para. 32; BerlKommTKG/*Klesczewski*, Section 110, para. 2.

[106] See BT-Drs. 16/2581, p. 28.

[107] BeckTKG-Komm/*Eckhardt*, Section 110, para. 94.

[108] See the Technical Directive TKÜV (TR TKÜV).

[109] BT-Drs. 15/2316, p. 94.

cc) Organisational obligations

The organisational and protective requirements are stipulated in Sections 12 to 17 TKÜV. Pursuant to Section 12 TKÜV, the telecommunication service provider must ensure that it has taken all necessary organisational steps for handling orders. In particular, it must also ensure that it can receive an order outside of its usual business hours without delay. Furthermore, it must ensure that it has competent personnel available at all times to answer enquiries from the authorised body.

Section 15 provides for confidentiality obligations concerning the way in which orders are implemented and requires that the protection of information related to interception measures be ensured. Pursuant to Section 16 Subsection 1 TKÜV, the telecommunication service provider must ensure that every application of its interception equipment is protocolled automatically and fully when the data necessary for the technical implementation are entered. According to Section 16 Subsection 2 TKÜV, the telecommunication service provider must ensure through technical configuration that personnel entrusted with the practical implementation of the interception have no access to the protocol data. Rules on the checking and deletion of protocol data, as well as on the destruction of documentation can be found in Section 17 TKÜV.

Furthermore, pursuant to Section 5 Subsection 5 TKÜV, the telecommunication service provider must inform the authorised body directly after the conclusion of the activities necessary for the technical implementation of an order of the point in time of actual setting up and of the identification actually carried out. This applies correspondingly to the transmission of information regarding the point in time of the termination of an interception measure. These provisions are especially of interest with regard to calculating the duration stipulated in the order.[110]

Sections 19 and 20 TKÜV specify the demonstration duties of Section 110 Subsection 1 No. 3 TKG, according to which the telecommunication service provider must demonstrate that his technical equipment and organisational arrangements meet the requirements of the TKÜV and of the TR TKÜV.

d) Protection obligations for the transmission of data by communication service providers

In line with Section 14 Subsection 1 TKÜV, the obligated party must provide state-of-the-art protection against unauthorised use of the technical equipment used to control the interception functions and the handover point, including the transmission paths between these.

---

[110] BeckTKG-Komm/*Eckhardt*, Section 110, para. 73.

Pursuant to Section 14 Subsection 2 Sentence 1 TKÜV, the copy of the intercept is to be protected by appropriate procedures against cognisance by unauthorised third parties. Procedures guaranteeing appropriate protection against transmission to unauthorised parties are to be applied when transmitting the copy of the intercept to the authority's recording lines. The corresponding necessary procedures are stipulated in more detail in the TR TKÜV. According to Section 14 Subsection 2 Sentence 7 TKÜV, the protective requirement of Section 14 Subsection 2 Sentence 1 TKÜV is regarded as fulfilled where the copy of the intercept is transmitted to the recording lines via dedicated transmission paths or via telecommunication networks with line-switching technology in light of the configuration principles underlying these transmission media.

e) Control, filter, and decryption obligations of communication service providers

Pursuant to Section 5 Subsection 2 TKÜV, the telecommunication service provider must provide the prosecution authorities with a full copy of the telecommunication which is conducted under the identification to be intercepted. In doing so, the telecommunication service provider must ensure that the data provided contains only the telecommunication referred to by the order, meaning, e.g., that only data from the timeframe specified in the interception order are provided.[111]

According to Part A, Annex G of the TR TKÜV, "broadcasting distribution services or similar services intended for the public (e.g., IPTV, Video on demand)" for which measures need not be taken pursuant to Section 3 Subsection 2 No. 4 TKÜV should as far as possible not be included in the intercept copy of an internet connection. Further filtering of content by the telecommunication service provider is, however, not envisaged. Instead, only the prosecution authorities are authorised to take note of the content of the intercepted communication;[112] Section 88 Subsection 3 Sentence 1 TKG prohibits service providers from obtaining knowledge of the content or circumstances of the telecommunication beyond the extent necessary for the commercial provision of their services.[113] Therefore all of the internet traffic routed through the intercepted line is extracted and forwarded to the prosecution authorities according to Section 5 Subsection 2 TKÜV.

---

[111] See BerlKommTKG/*Klesczewski*, Section 110, para. 43.

[112] BeckTKG-Komm/*Eckhardt*, Section 110, para. 31.

[113] Accordingly, a provider cannot be obliged to extract only specific IP data streams of a line for the authorised body's benefit. The precept of encroaching on the individual user's secrecy of telecommunication as little as possible does not constitute a violation of the ban on listening in on conversations pursuant to Section 88 TKG. See BGH, decision of 20 August 2015, Az. StB 7/15.

Also, there exists no obligation to decrypt encrypted communication.[114] Section 5 Subsection 2 TKÜV merely obliges telecommunication service providers to provide the authorities with a copy of the telecommunication to be intercepted.

6. Formal prerequisites of interception orders

a) Competent authorities

Pursuant to Section 100e Subsection 1 StPO, the telecommunication interception order can in principle be issued only by a court and only upon application by the public prosecution office. In exigent circumstances – in other words when one could expect the delay caused by waiting for a judicial decision to lead to the failure of the interception measure – the order may also be issued by the public prosecution office.

b) Requirements for applications

The law dictates no formal requirements for the public prosecution office's application. However, the competent judge must independently check whether the legal prerequisites for the requested measure are met. He is not bound by the investigative authorities' evaluation of the suspicious circumstances or of individual pieces of evidence while making his assessment. He must therefore be presented with all evidence relevant to the decision, and in complex cases with the investigation file as well. It is insufficient if the public prosecution office merely sums up and provides an evaluation of the main evidence in the application.[115]

c) Formal requirements for orders

According to Section 100e Subsection 3 StPO, the order is to be given in writing. This formal requirement is met when the order is issued by fax or email; however, in these cases, the original or a certified copy of the order must subsequently be provided within a week, Section 12 Subsection 2 TKÜV. The order has to indicate, where known, the name and address of the person against whom the measure is directed, the nature of the criminal charge underlying the order, the telephone number or other code of the telephone connection or terminal device to be intercepted, the nature of the information at which the measure is aimed, as well as the type, extent, and duration of the measure while specifying the time of its conclusion.

---

[114] BeckTKG-Komm/*Eckhardt*, Section 110, para. 72.

[115] BVerfG NJW 2016, 1781, 1786; BGH NJW 2010, 1297 (1298).

7. Substantive prerequisites of interception orders

a) Degree of suspicion

Section 100a Subsection 1 No. 1 StPO requires merely an ordinary degree of suspicion of someone having committed or participated in the commission of a serious criminal offence, or in cases where there is criminal liability for attempt, having attempted to commit such an offence or having prepared such an offence by committing a criminal offence. This suspicion must be founded on a sufficient basis of fact. This requires circumstances suggesting that someone has committed an offence or participated in the commission of an offence. The suspicion must have reached a certain degree of concretisation and substantiation founded on a coherent basis of fact.[116]

b) Predicate offences

Telecommunication interception pursuant to Section 100a Subsection 1 No. 1 StPO is an option only regarding certain serious criminal offences within the meaning of Section 100a Subsection 2 StPO (as listed in the annex below). Additionally, the deed forming the object of the investigation must be of some gravity in the individual case. For assessing this gravity, focus lies not on the likely sentencing range, but rather on an evaluative contemplation of the particular crime, with factors including the infringed legal interest's worthiness of protection, or a perpetrator's collaboration with other offenders.[117]

c) Persons and connections under surveillance

According to Section 100a Subsection 3 StPO, the interception measure can be directed against the accused or against persons of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their connection or information device.

The order may only be directed against *specific* persons.[118] As Section 100e Subsection 3 Sentence 2 No. 1 StPO shows, their identity need not yet be known at the time the interception order is issued. Where a targeted person's identity is not known, Section 100e Subsection 3 Sentence 2 No. 5 StPO stipulates that the order can simply indicate a certain telephone number or other code of identification for the targeted telephone connection or terminal device, in particular to an email box,

---

[116] BVerfG NJW 2007, 2749 (2751); BGH NJW 2010, 711.

[117] BVerfG NJW 2012, 833 (836); *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 11.

[118] *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 16.

a certain IP address, an IMSI, or IMEI.[119] However, giving the device number is only admissible when it can be ruled out that the same number is simultaneously assigned to another terminal device.[120]

d) Principle of subsidiarity

Section 100a Subsection 1 No. 3 StPO stipulates that telecommunication interception is permissible only when other means of establishing the facts or determining the accused's whereabouts would be significantly more difficult or altogether futile. A significantly greater degree of difficulty can be assumed particularly when much more time would have to be expended in order to investigate the offence absent the interception measure, leading to a considerable delay of the proceedings.[121]

e) Proportionality of interception in individual cases

Just as with any governmental encroachment on citizens' rights, a measure of telecommunication interception must also be proportionate in each individual case.[122] Proportionality can be negated particularly when a measure, while not expected to result *exclusively* in information related to the core area of privacy (in this case the measure would in any event be inadmissible pursuant to Section 100d Subsection 1 StPO), is likely to yield some information related to the core area of privacy. The degree of likelihood that information pertinent to the investigation can be obtained by the interception measure may also have an impact on the assessment of proportionality.

f) Consent to the measure by a communication participant

An order under Section 100a StPO is only dispensable when all parties to the communication have consented to the interception.[123] The situation when one party to the communication allows law enforcement officials to read or listen to the communication is not covered by Section 100a StPO. This concerns cases in which law enforcement officials gain knowledge of the communication's content in the way technically intended. This does not affect the communication procedure's confidentiality; it is only the trust which one communication participant may have placed in the other that

---

119 KK/*Bruns*, Section 100e, para. 14.

120 *Ibid*.; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100e, para. 14.

121 *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 13.

122 BerlKommTKG/*Klesczewski*, Section 110, para. 5; SK-StPO/*Rudolphi*, Section 100a, para. 13.

123 KK/*Bruns*, Section 100a, para. 3; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 1.

is disappointed.[124] Section 100a StPO safeguards the secrecy of telecommunication only against external third party access to remote communication. It does not cover the trust communication partners place in each other.[125]

8. Validity of interception order

a) Maximum duration of interception order

According to Section 100e Subsection 1 StPO, the court order of telecommunication interception shall be limited to a maximum duration of three months. An extension of up to three months at a time is admissible if the prerequisites for the order continue to exist, taking into account the information obtained during the investigation.

An order issued by the public prosecution office in exigent circumstances becomes ineffective if it is not confirmed by the court within three working days.

b) Prolongation of authorisation

An overall temporal limitation of the measure is not stipulated by the law, neither concerning the number of possible prolongations nor concerning the cumulative duration of interception. But if the measure produces no information supporting the underlying suspicion, then its necessity and thus its proportionality will appear increasingly questionable. There are no special formal requirements for the prolongation of authorisation.

c) Revocation of authorisation

When the prerequisites for issuing the order no longer prevail, Section 100e Subsection 5 StPO requires that measures implemented on the basis of the order be terminated without delay. The respective order can be revoked both by the public prosecution office and by the court.[126] A revocation is necessary particularly when the suspicion proves to be unfounded, the interception ceases to be indispensable for the investigation or it is no longer proportionate.[127]

---

124 BVerfG NJW 2002, 3619 (3620); NJW 2008, 822 (835).

125 BVerfG NJW 2008, 822 (835).

126 *Köhler*, in: Meyer-Goßner/Schmitt, Section 100e, para. 19.

127 *Ibid.*

9. Duties to record, report, and destroy

a) Duty to record and report

Personal data acquired through a measure of telecommunication interception are to be labelled accordingly, see Section 101 Subsection 3 Sentence 1 StPO. After conclusion of the interception, the court which ordered the measure is to be notified of its results according to Section 100e Subsection 5 Sentence 2 StPO. Reports on the measure's progress during its performance are not obligatory.

b) Duty to destroy

When personal data obtained through the measure are no longer necessary for the purposes of criminal prosecution or a possible court review of the measure, they shall be deleted without delay according to Section 101 Subsection 8 StPO. The fact of their deletion is to be documented. Not subject to deletion are chance discoveries unrelated to the measure's underlying procedure, but which are required as evidence for another criminal procedure and can be used for this purpose.[128] The decision on deletion is in principle made by the public prosecution office. The court decides once the case is pending.[129] Not only must the technical recordings of the interception be destroyed; the same applies to written records made.[130]

10. Notification duties and remedies

a) Duty to notify persons affected by the measure

The parties involved in the intercepted telecommunication are to be notified according to Section 101 Subsection 4 StPO. The notification is to be dispensed with where an affected person's protection-worthy overriding interests represent an obstacle thereto. This may be the case, for instance, when the measure has yielded no evidence incriminating the accused and the notification could prove damaging to his reputation with regard to his conversation partners.[131] The notification of a person not targeted by the measure can furthermore be dispensed with when this person was only insignificantly affected by the measure and where it can be assumed that he has no interest in being notified. This exception thus can only be applied to persons accidentally covered by the interception; it does not apply to the targeted persons.[132]

---

[128] *Ibid.*, Section 101, para. 27.

[129] *Ibid.*, para. 28.

[130] *Ibid.*, para. 28.

[131] *Ibid.*, para. 16.

[132] *Ibid.*, para. 17.

According to Section 101 Subsection 5 StPO, notification is to be made as soon as possible without endangering the purpose of the investigation, the life, physical integrity, and personal liberty of another person, or significant assets. Where a notification which had been deferred based on one of these reasons is not carried out within twelve months after completion of the measure, any further deferrals are subject to the court's approval according to Section 101 Subsection 6 StPO. The court may approve the permanent dispensation with notification where there is a probability bordering on certainty that the prerequisites for notification will not be fulfilled, even in future.

b) Remedies

As stipulated by Section 101 Subsection 7 StPO, the persons participating in intercepted communication may apply for a judicial review of the lawfulness of the measure, as well as of the manner and means of its implementation for up to two weeks following their notification. When an affected party gains knowledge of the measure, that person may file an application even before the measure's completion.

c) Criminal law consequences of unlawful interception measures

The unlawful eavesdropping or recording of non-publicly spoken words is subject to criminal sanctions under Section 201 StGB. The provision is also applicable to oral statements transmitted via telecommunication. For public officials, the provision provides for a higher sentencing range. If the statutory prerequisites of telecommunication interception are not fulfilled, then the acting official lacks authorisation, and, in consequence, faces criminal sanctions given the necessary intent. When the legal prerequisites for interception are not met and the individual acts with the necessary knowledge and intent, then public officials may also be held criminally liable concerning the transmission of non-spoken statements.

According to Section 202a StGB, whosoever unlawfully obtains access to data for himself or another that are not intended for him and are protected against unauthorised access, is criminally liable if he does so by circumventing the protection. This primarily concerns the unauthorised access to information systems by way of hacking.[133] However, data during their transmission are only covered by the provision when they are especially protected, in particular when they are encrypted.[134] As an unauthorised official interception order to a telecommunication service provider does not constitute a circumvention of special protection, no liability pursuant to Section 202a StGB ensues. However, Section 202b StGB also declares criminal-

---

[133] Schönke/Schröder/*Eisele*/*Lenckner*, Section 202a, para. 18; NK/*Kargl*, Section 202a, para. 12.

[134] NK/*Kargl*, Section 202b, para. 2.

ly liable whosoever unlawfully obtains data not intended for him, for himself or another by technical means from a non-public data transmission. Whether the data are especially protected (such as through encryption), is irrelevant. All forms of non-public electronic data transmission, in particular email, fax, VoIP, and internet chats are covered by the provision.[135]

d) Control by supervisory bodies

Furthermore, a non-judicial, independent supervision of interception measures can be performed by the respective data protection commissioners of the *Länder*, whose competency in these cases follows either explicitly from state provisions or from their general allocation of duties.[136]

11. Confidentiality requirements

a) Obligations of telecommunication service providers to maintain secrecy

According to Section 5 Subsection 4 Sentence 1 TKÜV, telecommunication service providers must ensure that the technical implementation of an interception order can be detected neither by the communication participants nor by third parties.

Pursuant to Section 15 TKÜV, the telecommunication service provider may not make available to unauthorised parties any information concerning the manner and means by which the interception orders are implemented by its telecommunication system (for instance concerning its interception concepts[137]). Furthermore, it has to ensure the protection of information relating to the interception measure. This applies particularly with respect to the unauthorised obtainment of information concerning the targeted IDs and the number of currently or previously targeted IDs.

b) Sanctions against telecommunication service providers and their employees

As obtaining knowledge of the content of intercepted telecommunication by the telecommunication service provider's employees is not permitted, they can also be held liable for eavesdropping on non-publicly spoken words according to Section 201 StGB. The unauthorised obtainment of knowledge concerning non-spoken statements may entail a criminal sanction for phishing under Section 202b StGB. Violating an obligation stipulated by Section 15 TKÜV (secrecy concerning the

---

[135] Schönke/Schröder/*Eisele*, Section 202b, para. 4; NK/*Kargl*, Section 202b, para. 2.

[136] An explicit provision can be found, e.g., in Section 34 Subsection 2 Sentence 1 BayDSG; pursuant to Sentence 2, the control is possible only after the conclusion of the investigative procedure and only if the collection of data was not reviewed by a court.

[137] BeckTKG-Komm/*Eckhardt*, Section 110, para. 79.

technical implementation of a measure) may be punished as a regulatory offence and can incur a fine of up to €500,000 pursuant to Section 149 Subsection 1 No. 22, Subsection 2 Sentence 1 TKG.

Moreover, when telecommunication is intercepted under Section 100a StPO, Section 17 Subsection 1 G 10 prohibits persons providing telecommunication services or contributing to the provision of such services from disclosing to other people the fact that telecommunication is being intercepted. Violating this obligation can be punished by up to two years in prison or a fine pursuant to Section 18 G 10.

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

a) Collection of traffic data

aa) Relevant information

Section 100g Subsection 1 StPO allows for the (long-term) collection of traffic data as defined in Section 96 Subsection 1 and Section 3 No. 30 TKG for the purpose of establishing the facts or determining the suspect's whereabouts. Hence, information such as the number or ID of the telephone connection or terminal devices concerned, personalised authorisation codes, or – when mobile connections are targeted – location data can be obtained, in principle in real time (see Subsection 1 Sentence 3) and thus without (further) recourse to Section 100a StPO being necessary.

In order to identify all mobile devices that were connected to a certain radio cell at a certain point in time Section 100g Subsection 3 StPO allows for prosecution authorities to also request all traffic data accrued with regard to that radio cell ("radio cell inquiry").

In addition, Subsection 2 StPO empowers prosecutors to access traffic data retained without occasion by telecommunication providers. At present, however, this instrument is de facto not available, after a court has found that aforementioned obligation of telecommunications providers under § 113b TKG in its current form violates EU law and the Federal Network Agency *(Bundesnetzagentur)* has since stopped enforcing named provision. The requirements for law enforcement authorities to access retained data as set out by the law and the current obstacles to the use of this power will be discussed in greater detail below (c.).

bb) Substantive prerequisites of collection

Collection of traffic data is only admissible when certain substantive prerequisites are met. Concerning the suspected crime, for instance, there must exist *cer-*

tain facts giving rise to the suspicion that the targeted person was involved in its commission (Subsection 1 Sentence 1) as perpetrator or participant (Sections 25 et seqq. StGB), and this criminal offence must furthermore be either of *substantial significance in the individual case*, Section 100g Subsection 1 Sentence 1 No. 1 StPO, or have been committed by means of telecommunication, Section 100g Subsection 1 Sentence 1 No. 2 StPO.

In the latter case, when an offence of non-substantial significance is concerned but this offence has been committed via telecommunication, however, no location data may be collected. This is due to the fact that Section 100g Subsection 1 Sentence 1 No. 2 StPO does not demand for a substantial significance of the case at hand that could justify the higher level of intrusion into the privacy of the person concerned that comes with the possibly long-term collection of location data. In cases of Subsection 1 Sentence 1 No. 2, also the subsidiarity clause in Subsection 1 Sentence 2 must be observed, meaning other means of establishing the facts would offer no prospect of success and the collection of data is proportionate to the importance of the case.

Radio cell inquiries pursuant to Subsection 3 are only permitted under the conditions of Subsection 1 Sentence 1 No. 1.

The necessary certainty of the facts requires that the suspicion goes beyond vague clues or mere conjecture.[138] In settled case law, the Federal Constitutional Court holds the element of "substantial significance" to be sufficiently clear for limiting the infringement of fundamental rights in criminal procedures.[139] Such offences are to be assumed when they exhibit at least an intermediate level of criminality, significantly disturb peace under the law, and could significantly compromise the population's sense of legal security.[140] Decisive for the classification as a crime of intermediate nature is the abstract sentencing range.[141] According to a decision by the Federal Constitutional Court, crimes punishable by a maximum sentence of under five years of imprisonment do not necessarily constitute crimes of substantial significance.[142] In such cases, the circumstances of the individual case are decisive.[143] Misdemeanours punishable by not more than two years, however, should never constitute a criminal offence of substantial significance.[144]

---

[138] BVerfG NJW 2007, 2749 (2751); BGH NStZ 2010, 711; *Köhler*, in: Meyer-Goßner/Schmitt, Section 100a, para. 9.

[139] See only BVerfG NJZ 2005, 1338, 1339.

[140] BVerfG NJW 2009, 2431, 2435; BVerfG NJW 2005, 1338, 1339; BVerfG NJW 2004, 999, 1010.

[141] BGH StV 2013, 1, 3, para. 31.

[142] BVerfG NJW 2009, 2431, 2435.

[143] BGH StV 2013, 1, 3, para. 31.

[144] *Köhler*, in: Meyer-Goßner/Schmitt, Section 98a, para. 5 with further references.

cc) Formal prerequisites of collection

The formal prerequisites of measures according to Section 100g StPO are laid out in Section 101a StPO. Its Subsection 1 Sentence 1 refers to Section 100a Subsections 3 and 4 (see supra III.B.7.c.) and Section 100e StPO (see supra III.B.6.). In particular, this means that the judge is competent for issuing the order, Section 100e Subsection 1 Sentence 1 StPO. The order must meet certain requirements. In particular, the judge must set out, on a case-by-case basis, the main considerations regarding the necessity and appropriateness of the measure, including the scope of the data to be collected and the period for which they are to be collected, Section 101a Subsection 2 and Section 100e Subsection 3 StPO. Its period of validity is to be limited to no more than three months, although this can be extended (Section 100e Subsection 1 Sentences 4, 5 StPO, cp. supra III.B.8.). Because of the reference to Section 100a Subsection 3 StPO, the order may only be issued with regard to telecommunication devices registered in the suspect's name, or in the names of persons it may be assumed function as a messenger for the accused, or that the accused is using their connection (see supra III.B.7.c.).

Measures pursuant to Section 100g StPO are generally to be performed in an open manner. The persons concerned must therefore be informed of the data collection. This may only be omitted if and as long as this would endanger the purpose of the investigation, Section 101a Subsection 6, Section 101 Subsection 4 Sentences 2 through 5 and Subsections 5 through 7 StPO.

dd) Duty of addressees to disclose information

Telecommunication service providers are required to cooperate pursuant to Sections 101a Subsection 1 Sentence 1, 100a Subsection 4 StPO (see supra III.B.5.).

ee) Automated procedure of disclosure

An automated procedure of disclosure for traffic data does not exist.

b) Collection of subscriber data

aa) Relevant information

For purposes of establishing the facts of a case or for determining the whereabouts of an accused person, subscriber data can be requested according to Section 100j StPO. Subscriber data as defined by the TKG are data concerning the contractual relationship itself (Sections 95, 3 No. 3 TKG), and, pursuant to Section 111 TKG certain data to be collected by the telecommunication service providers at the beginning of a contractual relationship prior to the activation specifically for the benefit of information requests made by the authorities – such as

telephone numbers, names connected to email addresses, dates of birth, the (international) mobile equipment identity number [IMEI], the (international) mobile subscriber identity number [IMSI] stored on the SIM-card, or *static* IP addresses.[145]

Requests for *dynamic* IP addresses are not covered by Section 111 TKG, as the "other connection codes" to be collected pursuant to Section 111 Subsection 1 Sentence 1 No. 1 TKG must be permanently assigned to a telephone subscriber.[146] This means law enforcement authorities may not request the changing IP-addresses assigned to a certain person to be disclosed to them. They may, however, based on Section 100j Subsection 2 StPO request subscriber data correlating with a known IP address, therefore enabling them to "decrypt" the dynamic IP addresses and identify its holder. The reference in Section 100j Subsection 2 StPO and Section 113c Subsection 1 No. 3 TKG clarifies that telecommunications providers may use the data to be retained by them under Section 113a TKG for the purpose of identifying the holders of dynamic IP addresses.

By reference to Section 113 Subsection 1 Sentence 2 TKG 100j Subsection 1 Sentence 2 StPO also covers request for "data, by means of which the access to terminal devices or storage media installed in these terminal devices or physically separate therefrom, is protected". This includes, in particular, the PIN and PUK of a SIM-card, as well as passwords for online data storage systems (especially cloud services).

bb) Prerequisites of data collection

In contrast to Section 100g StPO, there are no elevated material prerequisites for information requests under Subsection 1 or 2 relating to the suspicion of crime or concerning the significance of the individual offence.

Only regarding data that allow access to terminal or storage devices, Section 100j Subsection 1 Sentence 2 StPO stipulates that information may only be requested if the statutory prerequisites for the use of the data are met. This is the case, for instance, when physically separate storage media are to be accessed during a court-ordered search pursuant to Section 110 Subsection 3 StPO, or when emails stored in an email account are to be accessed by way of an overt access measure pursuant to Sections 94 et seqq. StPO.[147]

Also, the requirement of a court decision in Subsection 3 Sentence 1 must be heeded in these cases. In exigent circumstances, the order may also be issued by the public prosecution office or its officials working in the police force, although a

---

[145] KK/*Bruns*, Section 100j, para. 2.

[146] BeckTKG-Komm/*Eckhardt*, Section 111, para. 13.

[147] *Bär*, MMR 2013, 700, 703.

court decision must still be made afterwards without delay, Section 100j Subsection 3 Sentence 3 StPO.

Requests pursuant to Subsection 2 (personal information regarding dynamic IP addresses) are limited to isolated IP assignments at a specific point in time. Long-term assignments of (unknown) varying IP addresses to (known) subscribers (reverse situation of Section 100j Subsection 2 StPO), are possible only under Section 100g StPO.

cc) Duty of addressees to disclose information in manual and automated procedures

According to Section 100j Subsection 5 Sentence 1 StPO, any person providing or contributing to the provision of telecommunication services on a commercial basis can be an addressee of the aforementioned measures. Section 113 TKG authorises this person to transmit the aforementioned data to the investigation authorities in a manual procedure.

Alongside it, there exists an automated procedure of disclosure which is limited to data to be collected pursuant to Section 111 Subsection 1 Sentence 1 and Subsections 2, 3, and 4 TKG. In this procedure, the prosecution authorities (cp. Section 112 Subsection 2 No. 1 TKG), among others, can instruct the Federal Network Agency to access the available data and to transmit them to the requesting authority, Section 112 Subsection 4 Sentence 1 TKG.

c) Telecommunication data retention

An obligation to retain traffic data for a certain period was introduced into the TKG (Section 113a) by the legislature in 2007 while implementing Directive 2006/24/EG. However, the provision was declared null and void by the Federal Constitutional Court in its decision from 2 March 2010 due to constitutional deficiencies.[148] Later, also the directive which the provision was based on was declared invalid by the ECJ.[149] Nonetheless, in October 2015, the *Bundestag* passed the "Law for the implementation of a retention obligation and a maximum retention period for traffic data," which has been in force since 18 December 2015, thereby once again providing for the unoccasioned retention of traffic data for a certain period, Section 113b TKG. Also regarding the new provision doubts concerning the compatibility of the new provisions with EU law were voiced, soon.[150] However, the Federal Constitutional Court rejected issuing an emergency injunction.[151] It

---

148 BVerfG NJW 2010, 833.

149 EuGH NJW 2014, 2169.

150 *Boehm/Andrees*, CR 2016, 146 et seqq.; *Roßnagel*, NJW 2016, 533 (539).

151 BVerfG, ZUM-RD 2016, 701 and ZUM-RD 2016, 706.

must be pointed out, however, that the standard of review in the case of an emergency decision is different from that in the case of a decision on the merits. For an expedited decision, it is decisive whether – with respect to the respective consequences – it weighs more heavily to issue the order and afterwards the lawfulness of the challenged legal act is determined or whether, conversely, it weighs more heavily if the legal act turns out to be unlawful but may continue to be applied until the decision on the main action has been made. So far, no main decision has been rendered. However, de facto telecommunication providers currently are not required to respect their obligation under Section 113b TKG to retain certain traffic data without occasion. The background to this is the decision of the Münster Higher Administrative Court *(OVG)* in an urgent administrative procedure initiated by a provider, in which the court joined the criticism of § 113b TKG and declared the provision incompatible with the standards established by the ECJ in its judgment of 21 December 2016 in proceedings C-201/15 and C-698/15. There the ECJ clarified that Union law precludes a general and indiscriminate retention of traffic and location data. Nonetheless, the Member States were free, as a preventive measure, to provide for the retention of such data for the general purpose of combating serious crime. For this purpose, however, it would be necessary to limit data retention to the absolute necessary with regard to the categories of data to be retained, the means of communication collected, the persons concerned and the intended duration of the retention. Moreover, in order to avoid excessive data retention, the retention of data must always satisfy objective criteria which establish a link between the data to be retained and the objective pursued. These conditions would have to be particularly suitable to effectively limit the scope of the measure in practice and, consequently, the groups of persons concerned. Finally, national legislation must contain precise guarantees in order to protect the data against the risk of misuse. If this were observed, the EU Data Protection Directive would not stand in the way of a national regulation which would allow data to be retained in a targeted manner in order to combat serious crimes. The Münster Higher Administrative Court found that, in particular, the German provision permitting un-occasioned data retention, Section 113b TKG, did not define the required objective criteria suited to establish a link between the data and the objective pursued and, thus, did not limit the groups of persons concerned.[152] As a result of the Münster Higher Administrative Court's decision, the Federal Network Agency decided not to enforce the obligation under Section 113b TKG until further notice. Telecommunications providers are therefore still permitted to retain data, but do not have to fear any consequences if they do not comply.[153]

---

[152] For more, see BeckOK-StPO/*Bär*, 34th ed., 1 July 2019, Section 113 TKG recital 10 et seq.

[153] *Ibid*.

However, as Section 113b TKG has not been declared null and void by the Federal Constitutional Court, the concept of data retention will be presented below on the basis of the (principally) applicable provisions.

aa) Retention obligations

Pursuant to Section 113b Subsection 2 TKG, providers of publicly available telecommunication services (see supra III.B.5.a.) are required to retain, for a period of ten weeks, *inter alia*, the concerned telephone numbers or other IDs, the time, and the duration of all telephone calls (including the IP addresses involved as well as the assigned user ID in cases of VoIP). Furthermore, regarding mobile telecommunication, the retention obligation also covers the IMSI and IMEI, as well as the telephone numbers, and the time at which every SMS or MMS was sent or received.

Also to be retained for ten weeks according to Section 113b Subsection 3 TKG are a participant's assigned IP address, a definite connection ID, and an assigned user ID, as well as the time and duration of the respective internet use. Pursuant to Section 113b Subsection 4 TKG, the location data of users of mobile telephone or internet services must be retained for four weeks. Section 113 Subsection 5 TKG explicitly stipulates that the content of communication, data regarding the internet sites accessed, and data from electronic mail services may not be retained. Also, pursuant to Section 113 Subsection 6 TKG, the retention of traffic data may not cover connections to lines of telephone counselling services as per Section 90 Subsection 2 TKG.

Pursuant to Section 113c Subsection 2 TKG, data may not be transmitted for purposes other than the prosecution of particularly serious crimes, the prevention of concrete dangers to life, limb, or liberty of a person or for the continued existence of the Federal Republic of Germany or one of its states *(Länder)*, or for the purpose of subscriber data disclosure on the basis of Section 113 Subsection 1 Sentence 3 TKG, in which an IP address is used to determine the line assigned to it at a certain point in time. According to Section 113c Subsection 3 TKG, these data must be marked in such as fashion that it is distinctly recognisable that one is dealing with data retained pursuant to Section 113b TKG.

bb) Access to retained data

Accessing data retained pursuant to Section 113b TKG is subject to substantive prerequisites, the level of which is comparable to that of the conditions for acoustic residential surveillance under Section 100c StPO. Pursuant to Section 100g Subsection 2 Sentence 1 StPO traffic data may be accessed when certain facts give rise to the suspicion that a person, either as perpetrator or participant, has committed a serious criminal offence as stipulated in Section 100g Subsection 2 Sentence 2

StPO (or has attempted to commit such an offence, as the case may be), the offence constitutes one of particular gravity in the individual case and other means of establishing the facts would be much more difficult or offer no prospect of success, and the collection of the data remains proportionate to the significance of the case. The list of offences in Section 100g Subsection 2 Sentence 2 StPO roughly resembles that of Section 100c Subsection 2 StPO.

Section 100g Subsection 4 StPO also prohibits accessing traffic data that concerns persons subject to professional secrecy according to Section 53 Subsection 1 Sentence 1 Nos. 1 to 5 StPO that could be used to gain insights regarding which these persons could refuse to testify.

Concerning formal prerequisites, Section 101a Subsection 1 StPO refers to Section 100a Subsections 3 and 4 StPO (see supra III.B.7.c.) and Section 100e StPO (see supra III.B.6.), but, in the case of Section 100j Subsection 2, without the possibility of the public prosecution office issuing an order in exigent circumstances. Such a possibility only exists for traffic data to be accessed pursuant to Section 100g Subsection 1 StPO.

Pursuant to Section 101a Subsection 4 StPO, data accessed under Section 100g Subsection 2 StPO may be disclosed to other entities only to the extent that this is for purposes for which accessing the data would have been directly permissible as well. Concerning duties of notification, Section 101a Subsection 6 Sentence 1 StPO states as a rule that the persons concerned by measures pursuant to Section 100g StPO must be notified. By reference to Section 101 Subsection 4 Sentences 2 through 5 and Subsections 5 through 7 this may be delayed, however, or, under certain circumstances even be omitted, if the notification would endanger the purpose of the investigation. Aforementioned delay or omission of notification underlies judicial review and may only be ordered by a judge.

Aforementioned prerequisites, however, do not apply in so far as Section 100j Subsection 2 StPO, by referring to Section 113c Subsection 1 No. 3 TKG, permits telecommunications providers to use the retained data to be stored pursuant to § 113b TKG for the purpose of assigning dynamic IP addresses to their respective holders. In so far the prerequisites discussed under III.C.1.b.bb. apply.

2. Determination of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

a) Determination of device ID with the help of IMSI-catchers

Section 100i StPO regulates the collection of position and location reports sent by mobile terminal devices. The provision has been specifically designed for the use of so-called IMSI-catchers but has also been formulated in a technologically

neutral way, thus, principally permitting the use of other technical means to acquire aforementioned data.

By simulating a (fake) network cell for the mobile devices located within a certain radius, IMSI-catchers can enable the capture of the IMSI and IMEI numbers of unidentified mobile phones (under Section 100i Subsection 1 No. 1 StPO).[154] Alternatively, the location of a mobile phone within the radius of a network cell can be determined (under Section 100i Subsection 1 No. 2 StPO).[155]

Concerning the substantive prerequisites of an order, see the remarks on Section 100g StPO; the same goes for the investigation objectives and the formal prerequisites (both supra III.C.1.a.cc.). The prerequisites are largely the same. In contrast to Section 100g (and Section 100a) StPO, however, the order is to be limited to a maximum duration of six months under Section 100i Subsection 3 Sentence 2 StPO. Where third party personal data is concerned, the subsidiarity clause in Section 100i Subsection 2 Sentence 1 StPO must be observed.

b) Location determination via "silent SMS"

Mobile phones regularly disclose their location in the mobile network in order to be accessible. To ensure this accessibility, the network requires knowledge only of the so-called location area, made up of a variable number of network cells which cover an equally variable geographic surface.[156] Such a rough determination of location, which can be obtained as a traffic datum according to Section 100g StPO, is frequently insufficient for investigation purposes.[157] The exact network cell, however, is not identified until an active connection is established.[158] To induce such an active connection, "silent SMS" are used. They remain hidden from the mobile phone's user, but trigger the generation of the desired cell-specific traffic data again accessible on the basis of Section 100g StPO. "Silent SMS" play a significant role in (not only repressive) police (and intelligence) work. In the first half of 2018 alone, the Federal Office for the Protection of the Constitution, the Federal Criminal Police Office, and the Federal Police sent a combined 173,202 "silent SMS."[159]

---

154 *Hegmann*, Beck-OK StPO, Section100i, para. 1.

155 *Ibid*. para. 5.

156 Wikipedia, Location Area, accessible at http://de.wikipedia.org/wiki/Location_Area [as of 3 November 2019].

157 *Graf*, Beck-OK StPO, Section 100a, para. 132.

158 Wikipedia, Location Area, accessible at http://de.wikipedia.org/wiki/Location_Area #Ortung_im_Mobilfunknetz [as of 3 November 2019].

159 Wikipedia, Stille SMS, accessible at https://de.wikipedia.org/wiki/Stille_SMS #Datenschutz_und_Funkzellenermittlung_in_Deutschland [as of 3 November 2019].

After a long dispute over the statutory basis for this forced generation of traffic data, the BGH in its decision from 8 February 2018 – 3 StR 400/17 – ruled that such measures may be based on Section 100i Subsection 1 No. 2 StPO.[160] At least in practice, the question should thus be resolved.

D. Access to (Temporarily) Stored Communication Data

1. Online searches by means of so-called remote forensic software

a) Overview

For several years rules on access to information systems were only to be found in the preventive federal and some *Länder's* police laws for purposes of averting danger. The preventive police law provisions authorise general access to information systems ("online search" and "online surveillance"), and – as a special case – the surveillance and recording of telecommunication in such systems ("source telecommunication surveillance").[161] Since August of 2017 with Section 101b also the StPO contains a provision permitting (merely) "online searches" for the purpose of criminal prosecution. "Online searches" are not to be confused with "source telecommunication surveillance" despite, from a technological point of view, both measures can be executed using different functions of the same software. "Source telecommunication surveillance," however, is subject to Section 100a StPO as discussed above.[162]

b) Material prerequisites

"Online searches" as one of the most intrusive measures permitted by criminal procedural law is subject to the same material prerequisites as acoustic surveillance of private premises under Section 100c StPO.[163] In either case it is necessary that certain facts give rise to the suspicion that a person, either as perpetrator or participant, has committed a particularly serious criminal offence as, in the case of "online searches" stipulated in Section 100b Subsection 2 StPO (or has attempted to commit such an offence, as the case may be), the offence constitutes one of particular gravity in the individual case and other means of establishing the facts or the

---

[160] BGH NStZ 2018, 611, 613.

[161] Powers to perform online searches exist, e.g., in Rhineland-Palatinate, Section 31c POG RP, Bavaria, Article 45 BayPAG, and for the Federal Criminal Police Office in Section 49 BKAG. Regarding source telecommunication surveillance, see above III.B.2.c.

[162] III.B.2.c.aa.

[163] *Sieber/Brodowski*, in: Handbuch Multimedia-Recht, part 19.3 para. 159.

whereabouts of the person accused would be much more difficult or offer no prospect of success.

The measure may generally only be ordered against the person accused of the crime. Only if, on the basis of certain facts, it can be assumed that the accused herself uses the computer system to be intruded and that the intrusion into the systems of the accused will not suffice for establishing the facts or the whereabouts "online searches" may also be ordered against third parties (Section 100b Subsection 3 StPO).

c) Formal prerequisites

The formal prerequisites for measures under Section 100b StPO are governed by Section 100e StPO. Its Subsection 2 stipulates that "online searches" may be applied for by the prosecutor's office but may only be ordered special chambers of certain higher regional courts. Also in exigent matters a judge's order is required.

As in the case of telecommunication interception, special protection of information pertaining to the core area of privacy is accorded by Section 100d StPO.[164] According to Subsection 3, technical means shall be employed to ensure that data concerning the core area of privacy are not captured. Findings made on the basis of an online search which concern the core area of privacy shall be deleted without delay or submitted to the court ordering the measure by the public prosecution office for a decision as to their usability and deletion.

Orders may only be issued for the duration of one month but can be prolonged for one month each, if necessary.

Due to the reference to Section 100a Subsections 5 and 6 StPO in Section 100b Subsection 4 StPO technical safeguards must be put in place to ensure that the software used to intrude the target's computer cannot be abused by third parties and that secured data from the target's computer system is protected against alteration, unauthorized deletion and unauthorized access.

d) Use of data obtained for other proceedings

As explained supra a. data from online searches and similar measures can also be obtained under the states' police laws for preventive purposes. In accordance with Section 100b Subsection 6 No. 3 StPO such information may be exploited for *evidentiary purposes* or as *investigative clues* in criminal proceedings if an "online search" under Section 100b StPO could have been ordered. The same applies for information originally obtained through "online searches" under Section 100b

---

[164] On the resulting limits, see above III.B.3.a.bb.

StPO if they are to be used in other criminal proceedings, Section 100e Subsection 6 No. 1 StPO.

It is also permitted to use information accrued from measures under Section 100b StPO for preventive police purposes, Section 100e Subsection 6 No. 2 StPO, if the information are necessary especially to defend against immediate threats to life, limb or liberty of a person or to the existence of the state.

2. Search and seizure of stored communication data

a) Overview

Thus far, the system of rules on search and seizure has hardly been adapted to the requirements of the digital age. Due to a lack of alternatives, the existing procedural instruments must be used. Regarding the search for electronic (communication) data, these are the rules on the search of private premises, persons, and objects for the purpose of discovering evidence, Sections 102 et seqq. StPO. With respect to permanently securing or seizing data the relevant provisions include, on the one hand, the general rules on seizure in Sections 94 et seqq. StPO, which are tailored to apply to tangible objects, as well as the corresponding special provisions on the seizure of postal items pursuant to Sections 99 et seq. StPO, and, on the other hand, the regulations authorising the surveillance of intangible telecommunication in Sections 100a et seq. StPO.

However, the differentiation between tangible and intangible plays no role when it comes to the question of which statutory powers of intervention apply to which cases. Rather, it is the mode of the intervention (isolated/long-term and open/clandestine) and whether an encroachment on ongoing telecommunication is to take place that are decisive, as Section 100a StPO functions as *lex specialis* in these cases (for more, see below c.).

b) Search for electronic data

aa) Examination of electronic data, Section 110 Subsection 1 StPO

Searches may be performed in respect of the suspect (Section 102 StPO) as well as in respect of other persons (Section 103 StPO). *Inter alia*, objects belonging to a person may be searched. This includes computers and other data storage devices.[165] Usually, however, it will not be the computer or the data storage device itself that are of interest, but the data they contain. This makes it necessary to begin by sifting through the often vast amounts of data, first, in order to find out whether the sought-after data are on the computer or data storage device at all, and, second, in order to

---

[165] *Hegmann*, Beck-OK StPO, Section 102, para. 13.

narrow down the available data to only the relevant files. A seizure of the entire computer and all of its data would usually be disproportionate (see below c.aa.).

For this reason, the public prosecution office and, if it so orders, the officials assisting it, may examine documents during the search with regard to their relevance, pursuant to Section 110 Subsection 1 StPO. The term "documents" here includes all written thought content, regardless of its physical form.[166] Thus, electronic data also constitutes "documents" under the provision.[167] For the purpose of examination, the documents may furthermore be provisionally secured and removed from the premise;[168] regarding electronic data, this means a digital copy may be created. Nevertheless, securing hardware is also permissible when this is necessary for the examination.[169]

Section 110 Subsection 1 StPO is meant to safeguard personality rights and preclude the excessive, long-term collection of data.[170] By limiting the right of examination and selection to certain persons (prosecution office and the officials assisting it), one hopes to prevent extensive exposure of thought content to the broad access of investigators before the seizure has been effected.[171] However, the protection of personality rights appears imperfectly implemented when it comes to provisionally securing data pursuant to Section 110 Subsection 1 StPO, as the legal provisions fail to provide for procedures ensuring that knowledge of the measure is obtained not merely by the document-holder directly affected by the search (thus allowing him to seek legal recourse), but that persons whose rights are impacted by the content of the documents, are – at least in special cases – also notified and thus enabled to seek legal review. The problem arises, e.g., concerning the seizure of emails stored with the provider regarding the email account user or, more generally, regarding the sender and the recipient. The issue shall be dealt with in greater detail when discussing possibilities of open and clandestine collection of data (below e.).

bb) Examination of physically separate data storage media, Section 110 Subsection 3 StPO

Section 110 Subsection 3 StPO contains the only special power of intervention regarding electronic data found in the rules on search and seizure. The provision's purpose is to prevent potential loss of evidence. It stipulates that the search may be

---

166 BVerfG NStZ 2002, 377 (378); BGH CR 1999, 292 (293); KK/*Bruns*, Section 110, para. 2

167 *Ibid*.

168 BGH NStZ 2003, 670 (671); KK/*Bruns*, Section 110, para. 4.

169 BVerfG NStZ 2002, 377; *Park*, Handbuch Durchsuchung und Beschlagnahme, recital 818.

170 *Park*, Handbuch Durchsuchung und Beschlagnahme, para. 817.

171 *Ibid*. For comprehensive criticism of the provision, see *ibid.*, paras. 267 et seq.

extended to cover storage media physically separate from the location of the search – such as servers in the intranet or internet. However, this is only permitted under the condition that they are accessible from the storage medium found, e.g., by means of passwords found on location.[172] Whether the person concerned by the search is entitled to do so is irrelevant.[173] There must be a concrete danger of losing evidence (Section 110 Subsection 3 Sentence 1 StPO) which is the case when the external storage medium cannot be seized in time.[174]

Measures pursuant to Section 110 Subsection 3 StPO often have bearing on third parties. In this respect, the question already posed in aa) becomes relevant: to what extent must the measure be made known and in what way can third parties seek legal recourse? In contrast to cases of examination under Section 110 Subsection 1 StPO, Section 110 Subsection 3 Sentence 2 Hs. 2 StPO refers to Section 98 Subsection 2 StPO, which grants every person concerned (regarding the provision's original scope of application: by the seizure) the possibility of applying for a court decision. This shall be discussed in more detail in d.).

The access to external storage devices also poses problems with regard to such devices often not being located in Germany, but in foreign countries – without that fact being simple to determine.[175] Thus the question arises under which conditions other nations' sovereign rights are compromised by accessing storage media located abroad, thereby leading to the necessity of requesting mutual legal assistance. As far as can be seen, no relevant case law yet exists. In the applicable commentaries, these open questions are frequently not discussed adequately; instead, a solution is often proposed with hardly any supporting reasoning.[176]

---

[172] KK/*Bruns*, Section 110, para. 8.

[173] Such a restriction was rejected during the legislative process with reference to Section 98 Subsection 2 StPO, see BT-Drs. 16/6979, p. 45. Also note, however, that according to Article 32 lit. b of the Council of Europe Convention on Cybercrime, storage media located in another country may be accessed only with the "lawful and voluntary consent of the person who has the lawful authority to disclose the data […] through that computer system".

[174] *Hegmann*, Beck-OK StPO, Section 110, para. 13; *Park*, *ibid*., para. 825.

[175] See *Sieber*, Gutachten 69. Deutscher Juristentag, C 36.

[176] *Hegmann*, BeckOK StPO, Section 110, paras. 15 et seq.; *Köhler*, in: Meyer-Goßner/Schmitt, Section 110 paras. 7a et seq.; KK/*Bruns*, Section 110, para. 8a; *Park*, Handbuch Durchsuchung und Beschlagnahme, para. 7826. But see *Sieber*, Gutachten 69. Deutscher Juristentag, C 139 et seq., regarding the problems connected with a nation conducting independent transnational investigations.

c) Applicability of seizure provisions to electronic data

aa) Underlying principle

The traditional provisions on seizure in Sections 94 et seqq. StPO relate to (tangible) objects. However, constitutional and federal case law concurs that seizing storage media, including the data they contain, for use as evidence in criminal proceedings is also permissible on the basis of Sections 94 et seqq. StPO.[177] The principle of proportionality requires – *a maiore ad minus* – that the data storage media not be seized, but only the data they contain be secured to the extent this proves practically feasible.[178] Moreover, it must be ascertained that excessive data are not seized.[179]

bb) Collection of electronic data

The conditions under which stored electronic communication – such as emails on the provider's server – can be seized, has not been settled in every respect.

(1) Locally stored messages before, after, and during transmission

Cases, in which emails or messages to be transmitted by other means are still stored on the computer or mobile phone, e.g., in form of a draft, as well as cases in which they have been retrieved and subsequently saved locally, are unproblematic. Due to the absence of the specific risks Article 10 Subsection 1 GG is meant to afford protection against, they are not covered by the secrecy of telecommunication.[180] Thus, the same rules apply as for any other type of data and they can be seized pursuant to Sections 94 et seqq. StPO (see aa.).[181]

Also unproblematic are situations in which emails are in the process of transmission. This applies during the following phases: first, after having been dispatched by the sender and prior to arriving at the sender's provider; second, after having been dispatched by the sender's provider and prior to arriving at the recipient's provider; and third, during retrieval by the recipient. Since it is necessary to intervene in an ongoing telecommunication process in order to access the messages, only Section 100a StPO can serve as statutory basis for the intervention.[182]

---

[177] BVerfG NJW 2005, 1917 (1919); NJW 2006, 976; *Gerhold*, BeckOK StPO, Section 94, para. 4.

[178] BVerfG ZUM-RD 2005, 322 (330 et seq.).

[179] BVerfG NJW 2005, 1917 (1920 et seq.); NJW 2009, 2431 (2436, para. 81); BGH NStZ 2010, 345 (346).

[180] BVerfG NJW 2006, 976 (978 et seq.).

[181] See *Graf*, Beck-OK StPO, Section 100a, para. 53.

[182] *Ibid.*, para. 54.

(2) Communication data temporarily or permanently stored with third parties for the purpose of further transmission or safekeeping

Also settled is the question of isolated open access to emails stored with the recipient's provider. The Federal Constitutional Court declared such access permissible on the basis of Sections 94 et seqq. StPO. The issue had previously been disputed both regarding its constitutional and its criminal procedural dimensions.[183] Topics of this discussion included the intertwined questions of to what extent emails temporarily or permanently stored with the provider fall under the scope of the secrecy of telecommunication, and whether Sections 94 et seqq. StPO can even justify an encroachment on the secrecy of telecommunication. Many were of the opinion that the criminal procedural powers of intervention contained in the eighth chapter of the StPO related to specific encroachments on fundamental rights, and that these encroachments could be justified only on the basis of the corresponding provisions in the StPO. Thus, according to widespread opinion, encroachments on Article 10 Subsection 1 GG could only be based on Sections 99 and 100a StPO (as well as Section 100g StPO which is, however, not of relevance for the cases at hand).[184] They allow for clandestine access to ongoing communication, since the person concerned has no means of monitoring activities beyond his sphere of control. Pursuant to this view, on the one hand, these invasive measures constituted statutory realisations of the specific dangers that Article 10 Subsection 1 GG is to protect against. On the other hand, encroachments could only be justified under the material and formal conditions stipulated in these provisions, including adherence to the respective procedures.[185]

In its 2009 decision quoted above, the Federal Constitutional Court held that the specific dangers of spatially distanced communication, which Article 10 Subsection 1 GG is intended to provide protection against, only apply to data until such time as the party concerned gains exclusive control over the contents of his mail box.[186] Furthermore, it held that Sections 94 et seqq. StPO satisfied the constitutional requirements for *open and isolated* encroachments on the secrecy of telecommunication.[187] It also declared that Sections 99, 100a and 100g StPO did not

---

[183] BVerfG NJW 2009, 2431 et seqq.

[184] Thus, specifically regarding the possibility of seizing emails at the provider based only on Section 100a StPO, e.g., LG Hamburg MMR 2008, 186 et seq.

[185] Regarding Section 100a StPO as a "conclusive regulation" cp. *Löwe/Rosenberg/Schäfer*, Section 100a (as of 1 April 1986), para. 5, according to which Section 100a StPO essentially differs from Section 99 StPO in that the former permits the interception of future, transient telecommunication, while Section 99 applies to earlier, fixed telecommunication, *ibid*., Section 99, paras. 2 et seq.

[186] BVerfG NJW 2009, 2431 (2433, para. 46).

[187] BVerfG NJW 2009, 2431 (2432 et seq.).

constitute *leges speciales* conclusively regulating such encroachments on the fundamental right.[188]

Yet even after this decision, uncertainties remain in cases in which communication is accessed without knowledge of the person concerned – possibly for an extended duration – by performing the interception at third parties employed by the person concerned for the further transmission or non-local storage of their messages. This relates to cases, e.g., in which emails are accessed which are temporarily or permanently stored with the recipient's provider or that are cached briefly with the sender's provider for onward transmission.[189] For encroachments of this kind, an application of Section 99 or Section 100a StPO can be considered. The two provisions differ markedly in their substantive prerequisites, as well as in their procedural requirements.[190] The question of which is applicable is of practical relevance, since it is not always possible to seize messages at the recipient's provider. If a suspect sends an email to a location beyond German jurisdiction where (timely) mutual legal assistance is not available, it can prove necessary to collect the data at the sender's provider during the brief phase of cache storage, i.e., after arrival and prior to onward transmission. This would require a statutory power of intervention permitting not merely isolated access to data present at a certain time, but to first extract *all* emails for closer examination regarding their relevance and, when necessary, to seize them.

The issue has not yet been explicitly brought before the Federal Constitutional Court for clarification, and there is disagreement between the lower courts regarding which solution is preferable.[191] However, in the Federal Constitutional Court's considerations underpinning its ruling on Sections 94 et seqq. StPO, the court formulated criteria by which the invasiveness of not only isolated and open, but also of long-term and secret seizures of communication data are to be assessed. Correspondingly, it also outlined the requirements for a statutory empowerment permitting these measures in such a way that one can at least identify provisions which clearly fail to meet these standards. In this respect, the decision continues along traditional lines in that it places stringent requirements on the justification of (pos-

---

[188] BVerfG NJW 2009, 2431 (2433 et seq., paras. 57 et seq.).

[189] Regarding the seven phases of an e-mail transmission, see *Graf*, Beck-OK StPO, Section 100a, para. 53.

[190] Advocating an application of Section 99 StPO: AG Reutlingen, decision of 31 October 2011, Az. 5 Ds 43 Js 18155/10 jug; apparently also LG Hildesheim, decision of 21 April 2010, Az. 26 Qs 58/10; *Bär*, MMR 2013, 700 (703). By contrast, proponents of Section 100a StPO: LG Landshut, decision of 21 May 2012, Az. 6 Qs 82/12 (however, no general rejection of Section 99 StPO, see para. 16 of the decision); *Köhler*, in: Meyer-Goßner/*Schmitt*, Section 100a, para. 6c; *Graf*, Beck-OK StPO, Section 100a, paras. 57, 64 ("for the interim"); *Klein*, NJW 2009, 2396 (2399). The often quoted decision BGH NJW 2009, 1828 was made prior to the decision of the BVerfG. Thus it cannot readily be held to still apply unreservedly.

[191] *Ibid*.

sibly long-term) clandestine encroachments on the fundamental rights of data protection due to the ensuing limitation of the concerned party's ability to avail itself of a legal remedy.[192]

Regarding the level of invasiveness, the Federal Constitutional Court held:

> "The gravity of an encroachment is greater when it ensues secretly […]. The long-term encroachment on ongoing telecommunication is more intensive than a one-off and isolated collection of data, since the scope and variety of the obtained data is considerably greater […]. The possibility of the collected data being used for unspecified or not yet specified purposes also increases the gravity of the encroachment – even at the stage of collection […]. Finally, the degree of invasiveness is higher when the affected person has no influence on the data concerning him or her […]."[193]

Correspondingly, there exist certain thresholds for taking action in the law of criminal procedure:

> "[…] For clandestine encroachments on the secrecy of telecommunication as well as for access to comprehensive data stocks retained without suspicion […] and upon which the person concerned has no influence, particularly stringent standards for access apply regarding the gravity of the investigated crime and the degree of suspicion necessary […]. Whereas regarding an open measure ensuing from a search, one which does not encroach ongoing communication and is limited to the investigation's purpose, such as seizing emails stored on the provider's mail server, the prohibition of excessiveness – in face of the level of the state's interest in criminal prosecution – does not require that the seizure of emails stored on the provider's mail server be permitted only for the prosecution of particularly serious criminal offences (such as in Section 100c StPO), serious criminal offences (such as in Section 100a StPO), or criminal offences of substantial significance (as in Section 100g StPO). In line with the conditions regularly applicable for criminal investigations, the initial suspicion of a crime having been committed may suffice for allowing prosecution authorities to access communication content, if this ensues outside of ongoing telecommunication and with knowledge of the person concerned – such as in the case seizures."[194]

Thus, only regarding measures of open, isolated search and seizure did the Federal Constitutional Court hold that – due to their relatively minor level of invasiveness – neither a special degree of suspicion nor a limitation to certain criminal offences was necessary. However, Section 99 StPO, which allows for secret access according to Section 101 Subsection 5 StPO (a subsequent notification can even be dispensed with entirely pursuant to Section 101 Subsection 6 Sentence 3 StPO), places no substantive restrictions whatsoever on encroachments. Substantively, the initial suspicion of having committed (any) criminal offence is enough. In line with the court's reasoning, the fact that Section 100 StPO stipulates more stringent procedural requirements compared to those applicable for the normal seizure pursuant

---

[192] See, e.g., BVerfGE 120, 274 (323 et seqq., paras. 234 et seqq.) (online search); BVerfG NJW 2003, 1787 (1791) ("Prerequisite is a criminal offence of substantial significance, a concrete suspicion of commission"); BVerfG NJW 1973, 891–893. This is also pointed out by *Klein*, NJW 2009, 2996 (2998).

[193] BVerfG NJW 2009, 2431 (2434, para. 68).

[194] BVerfG NJW 2009, 2431 (2434 et seq., para. 69).

to Section 94 StPO cannot compensate for this deficiency, as procedural precautions only serve an ancillary function to the substantive balancing of interests.[195] In light of this case law, applying Section 99 StPO in the aforementioned scenarios seems a constitutionally questionable proposal. Yet the Federal Constitutional Court gave no conclusive indications as to whether or not it would be permissible – at least during an interim period – for lower courts to modify Section 99 StPO in line with constitutional requirements (in addition to the usual assessment of proportionality that has to be made in every case) and thus essentially to craft a suitable empowerment in each individual case themselves.[196]

d) Different standards of protection for stored and for transmitted data

With regard to the statutory law, the conditions for an encroachment seem to depend on whether stationary data or data in transmission is supposed to be accessed. A seizure pursuant to Sections 94 et seqq. StPO may be performed subject to much less stringent conditions than an encroachment on ongoing telecommunication, which Section 100a StPO is tailored to.

However, pursuant to the Federal Constitutional Court's outlined decision, the required level of protective preconditions is not determined by whether stationary data or data in transmission are concerned. Rather, what is decisive according to the criteria mentioned above is whether an encroachment ensues openly and only isolatedly or whether it ensues secretly and possibly extends over a long duration of time, since in latter cases the court requires that higher standards be met regarding the gravity of the offence being prosecuted as well as regarding the degree of suspicion necessary. The legislature will have to use this as a guideline in an – urgently necessary – reform of the search and seizure provisions.

e) Open and clandestine access to stored data

Both searches pursuant to Sections 102 et seqq. StPO as well as seizures pursuant to Sections 94 et seqq. StPO principally constitute open measures. As a general rule, they both require a judicial order (Section 105 Subsection 1 Sentence 1 Hs. 1, Subsection 1 Sentence 2 Hs. 1 StPO, or Section 98 Subsection 1 Sentence 1 Hs. 1 StPO respectively), which entails a right to be heard pursuant to Article 103 Sub-

---

[195] Regarding the procedural requirements, see BVerfG NJW 2009, 2431 (2437 et seqq., paras. 92 et seqq.).

[196] Of this opinion, however, is *Bär*, who interprets the mention of Sections 99 and 100a StPO by the BVerfG NJW 2009, 2431 (2434, para. 58) not as a mere dismissal of a constitutionally relevant *lex-specialis*-relationship in favour of Sections 99 and 100a StPO (as the preceding para. 57 would suggest). At least for secret and long-term seizures of e-mails *Graf*, Beck-OK StPO, Section 100a, para. 57, in accordance with this author's reasoning, now also assumes that the seizure of e-mails must be measured against Section 100a StPO.

section 1 GG.[197] Entitled to this right is the person "whose (own) rights are infringed directly by the court order."[198] "Apart from those formally party to a procedure, this may also refer to the person substantively affected by the judicial decision."[199] Regarding content, this implies that a person thus formally or substantively concerned must be allowed to make a statement, and that his or her statements must be acknowledged and be taken into consideration.[200] So as not to undermine the right to be heard, the person concerned must be sufficiently heard prior to a decision.[201] Thus, the court must make sure that the procedure does not reach a stage in the decision-making process detrimental to the person concerned before that person has obtained knowledge of the procedure.[202]

This right, which is based on Article 103 Subsection 1 GG, has been implemented in statutory form, *inter alia* in Sections 33 and 35 StPO,[203] which also apply to judicial decisions on investigative measures. Thus, a person concerned must be given notice pursuant to Sections 33 Subsection 2, 35 Subsection 2 StPO of search and seizure orders, including the reasons given for the respective decision (see Section 34 StPO) by no later than the commencement of the measure.[204] However, the prior hearing demanded by Section 33 Subsections 3, 2 StPO can be dispensed with pursuant to Section 33 Subsection 4 StPO where it would endanger the success of the measure.[205] Moreover, it used to be common practice to withhold – based on an analogous application of Section 101 StPO, which regulates the procedure for the clandestine investigative measures exhaustively enumerated there – at least the reasons for the decision as long as their knowledge could endanger the investigation.[206] However, this case law has now been abandoned by the Federal Court of Justice *(Bundesgerichtshof)*.[207] Unlike Section 101 Subsection 5 StPO does with regard to the investigative measures listed in Section 101 Subsection 1 StPO the Code of Criminal Procedure does not provide for deferring the notification based

---

197 Regarding seizure, cp. BVerfG NJW 1965, 1171 et seq.

198 BVerfG NJW 1988, 1963. Regarding the Code of Criminal Procedure, see KK/*Maul*, Section 35, para. 3.

199 BVerfG NJW 1988, 1963. Regarding the Code of Criminal Procedure, see *Larcher,* Beck-OK StPO, Section 35, para. 2.

200 Maunz/Dürig/*Schmidt-Aßmann*, GG, 74. suppl. 2015, Article 103 para. 69.

201 *Ibid*., para. 92.

202 BVerfGE 36, 85 (88).

203 KK/*Maul*, Section 35, para. 1.

204 Regarding search, BGH NStZ 2003, 273 et seq.; BVerfG NJW 2009, 2431 (2437, para. 95); *Gerhold*, Beck-OK StPO, Section 98, para. 11.

205 This exception is constitutionally sound, see BVerfGE 100, 313 (361).

206 See BGH NStZ 2003, 273 (274) regarding the narrow limits of this possibility. See also BVerfG NJW 2009, 2431 (2437, para. 94), according to which it would be constitutionally unobjectionable even to withhold notice of the entire measure.

207 BGH NStZ 2010, 345 and BGH NStZ 2015, 704.

on an endangerment of the investigation's purpose regarding cases of seizure pursuant to Sections 94 et seqq. StPO.[208]

Yet, despite or rather because of the formal openness of aforementioned measures there are no rules in place to ensure that everybody concerned by a measure, esp. third parties, are informed of it. By contrast, comprehensive statutory regulation on procedure exists in Section 101 StPO regarding planned clandestine measures. This includes, *inter alia*, Sections 99 and 100a StPO (see Section 101 Subsection 1 StPO). The provision contains a differentiated system concerning the handling of personal data as well as who is to be notified at what point in time of the encroaching measures performed, and which options for subsequent legal recourse are available. For example, regarding a measure pursuant to Section 99 StPO the sender and the addressee of a postal item, and regarding a measure pursuant to Section 100a the participants in the telecommunication under surveillance are to be notified as soon as this can be effected, *inter alia*, without endangering the purpose of the investigation (Section 101 Subsection 4 Sentence 1 Nos. 2, 3, Subsection 5 Sentence 1 StPO). However, notifications can be dispensed with when a non-targeted person was only tangentially affected by the measure and it may be assumed that the person has no interest in being notified (see Section 101 Subsection 4 Sentence 4 StPO).

When compared to these well thought-out and concise provisions, the state of the law appears insufficient with regard to formally open measures.[209] The latter also frequently have secretive elements but the respective statutory provisions are, in contrast to the rules on clandestine measures, deficient with respect to the protective elements actually necessary with regard to the measures' frequent relevance to third parties' personality rights. Take the following examples: the seizure of emails at the provider concerns not only the provider as custodian, but also the user of the mail box as well as all other participants in the communication. This situation principally seems comparable to that of a measure pursuant to Section 100a StPO – only in contrast to Section 100a StPO, there exists no procedural provision comparable to Section 101 Subsection 4 Sentence 1 No. 3 StPO which stipulates the notification of the parties affected by the telecommunications surveillance.

Third party rights are also affected when, during a search, (communication) data – possibly after first securing them – are comprehensively combed through for their relevance, Section 110 Subsections 1, 3 StPO. Communication relationships protected by Article 10 Subsection 1 GG or at least by the (constitutional) right to informational self-determination could thereby be subjected to the investigators' scruti-

---

[208] *Ibid*. Since seizures frequently only form part of a whole bundle of measures the obligation to inform without delay can thus endanger ongoing measures, e.g., those pursuant to Section 100a StPO. Prosecutors therefore need to carefully coordinate their various measures.

[209] This discrepancy is also noted by *Brodowski*, JR 2009, 402 (407).

ny, even if they later turn out to be irrelevant. Moreover, the examination pursuant to Section 110 Subsection 3 StPO, for instance, grants the power to access shared drives which are not (solely) in the rightful power of disposition of the person concerned by the search, but are also used and furnished with data by third parties.

To the extent that the relevance to third parties is a consequence of a judicial decision, i.e., particularly in cases of seizure, the issue first comes up as one regarding the right to be heard. In accordance with the criteria mentioned at the beginning, one must thus determine when a third party is directly substantively affected. When this is the case, the third party must be notified of the decision pursuant to Section 35 StPO. This was held by the Federal Constitutional Court to necessarily apply to the user of a mail box seized at the provider.[210] However, the provisional securing and examination pursuant to Section 110 StPO is not based on a judicial decision, so that such a measure does not fall within the scope of protection of Article 103 Subsection 1 GG and Sections 33 and 35 StPO do not apply. To what extent the prosecution authorities need to take action regarding other persons affected, in particular whether these must also be informed so that they can have the respective measure reviewed by a judge, remains open and is left for the responsible public prosecutor to decide in the individual case. It would therefore be advisable for the legislature to confront the issue and to standardize the manner in which the potentially affected third party fundamental rights (in particular the right to information following from the data protection rights, the right to a judicial review following from Article 19 Subsection 4 GG and Article 103 Subsection 1 GG) are to be accorded procedural protection.[211]

3. Duties to cooperate: production and decryption of data

The German StPO contains no special provisions on the basis of which the investigative authorities could demand the decryption of encrypted data or the surrender of the passwords necessary for decryption. The general rules concerning duties of witnesses and the obligation of the (non-accused) custodian to surrender objects in cases of seizure are of limited expedience and require – sometimes significant – restricting modifications to ensure proportionality.[212] Pursuant to Sections 48 Sub-

---

[210] BVerfG NJW 2009, 2431 (2437, para. 94). *Brodowski*, JR 2009, 402 (407) appears to have overlooked this requirement stipulated by the court. Nevertheless, a direct seizure at the provider will likely be the exception. First, a seizure of the entire mailbox usually proves disproportionate, BGH NJW 2010, 1297 (1298, paras. 15 et seq.). Second, precisely specifying prior to an examination which data are to be seized will likely only be possible under exceptional circumstances.

[211] Regarding the relationship of Article 103 Subsection 1 GG to other provisions in the Constitution, see Maunz/Dürig/*Schmidt-Aßmann*, GG, 74. suppl. 2015, Article 103 paras. 6 et seqq. For the requirements concerning obligations to inform in the course of measures of criminal procedure, see esp. BVerfG NJW 2012, 833 (838 et seq.).

[212] Instructive: *Sieber*, Gutachten 69. Deutscher Juristentag, C 119–122.

section 1 Sentence 2, 161a Subsection 1 StPO, non-suspect witnesses are required to testify truthfully regarding their own perceptions. This may include testifying about any access codes known to them.[213] By using this method, the prosecution authorities could potentially gain extensive access to personal data without the method being subject to substantive limitations. Until a statutory regulation is introduced, *Sieber* therefore advocates closely tying such access to the intended utilisation and the ensuing respective prerequisites.[214] The option of issuing a so-called production order, entailing the obligation to provide data in plain text form, does not exist on the basis of the current body of law, in particular not on the basis of Section 95 StPO. The obligation to surrender applies only to objects already in a person's custody.[215]

IV. Use of Communication Data in Judicial Proceedings

1. Use of communication data in the law of criminal procedure

The German StPO includes no special provisions regarding the introduction of electronic data. In principle, the court decides in what way electronic data are introduced into the main hearing and how they are used (Section 244 Subsection 2 StPO). Yet regarding strict evidentiary proceedings *(Strengbeweisverfahren)*[216] the StPO provides only for evidence in the form of witness testimony (Sections 48 et seqq. StPO), expert opinions (Sections 72 et seqq. StPO), documents (Section 249 StPO), and inspections (Section 86 StPO). All of these may be of relevance when it comes to introducing electronic data or their content. This applies both for seized data as well as for data intercepted in the course of ongoing telecommunication. During an inspection, the collected data are made directly audible or visible in the main hearing with the aid of a computer monitor or a loudspeaker.[217] In cases of

---

213 *Ibid.*, p. 120.

214 *Ibid*., p. 121.

215 *Ibid.*, p. 121.

216 In the German law of criminal procedure, two different types of evidentiary proceedings may apply depending on which facts are to be ascertained and whether this is to ensue during the main hearing. In the main hearing, a strict evidentiary proceeding – with only certain forms of admissible evidence – applies when it comes to ascertaining the sequence of events fulfilling the elements of an offence, or regarding facts either relating to the defendant's guilt or which have an impact on the sentence. Outside the main hearing, or in the main hearing concerning facts other than those just mentioned, an open evidentiary proceeding applies. For more, see *Schmitt*, in: Meyer-Goßner/Schmitt, Section 244, paras. 6 et seqq.

217 BGH NStZ 2002, 493 regarding the introduction of conversation recordings into the main hearing.

documentary evidence, records or printouts of data are read out.[218] A supplementary hearing of the officer responsible for the data analysis as a witness can streamline the taking of evidence, particularly in cases where the amount of data concerned is vast.[219] Finally, experts can help the court assess the authenticity and integrity of data.

2. Inadmissibility of evidence as a consequence of inappropriate collection

a) Inadmissibility of evidence following the unlawful collection of evidence

Complicated legal issues arise when the prerequisites for collecting evidence are disregarded. It leads to the question of whether these unlawfully obtained pieces of evidence may still be admitted. On the one hand, this problem concerns the further utilisation during the investigative procedure, and on the other, it concerns their admissibility for evidentiary purposes during the main hearing. The correct way of handling these topics is subject to extremely contentious debate; the discussion of the issue is characterised by a myriad of academic papers and – sometimes contradictory – case law.[220] The following delineation shall – in line with the empirical nature of this study and the specific question posed – therefore confine itself to the basic principles of constitutional and federal court case law regarding the use of evidence in the main hearing.

Whether a conviction may be based on evidence obtained by way of procedurally unlawful coercive measures must be determined, e.g., when rights to refuse to testify or to answer questions are disregarded while gathering evidence. This scenario concerns cases, for instance, where suspects' or their defence attorneys' laptops are seized, containing files relevant to their criminal defence. Regarding the accused person, the prohibition of seizure follows from an analogous application of Section 97 Subsection 1 StPO in connection with Article 2 Subsection 1, Article 20 Subsection 3 GG.[221] The defence attorney's files are protected pursuant to Sec-

---

[218] *Graf*, Beck-OK StPO, Section 100a, para. 161.

[219] *Ibid.* This does not violate the principle of immediacy of Section 250 StPO. For Sections 250 et seqq. StPO merely stipulate when *personal* evidence may be substituted or supplemented by *documentary* evidence. It does not prohibit substituting or supplementing documentary evidence by personal evidence. Hearing the officer responsible for the analysis must therefore (merely) be consistent with the court's general duty to accurately ascertain the facts of the case pursuant to Section 244 Subsection 2 StPO, see *Roxin/Schünemann*, StPO, Section 46, para. 33. The lower evidentiary value of this testimony compared to the (direct) documentary evidence must, however, be taken into account when evaluating the evidence, *ibid*., para. 34.

[220] For more, see *Roxin*/*Schünemann*, StPO, Section 24, paras. 13–67.

[221] BGH NStZ 1998, 309 (310). Concerning the seizure of a laptop of which the suspect claims it contains files relevant to her defence, see BVerfG NStZ 2002, 377 et seqq.

tions 97 Subsection 1 Nos. 1, 2, 53 Subsection 1 Sentence 1 No. 2 StPO. The question whether unlawfully collected evidence may be admitted also arises, e.g., when telecommunication interception under Sections 100a et seq. StPO is ordered without the necessary suspicion of a serious criminal offence pursuant to Section 100a Subsection 2 StPO having been committed, or when the order is issued by the public prosecution office despite the absence of exigent circumstances.

However, a ban on the admission does not automatically follow from such violations if the inadmissibility of evidence is not explicitly provided for by law – which it only exceptionally is (for instance, in Section 136a Subsection 3 Sentence 2 StPO). A ban on the admission of evidence "constitutes, from a constitutional point of view, an exception requiring grounds to be given" as it "impairs the ascertainment of a substantively correct and fair decision."[222] Thus, according to established case law of the Federal Court of Justice and the Federal Constitutional Court, a weighing of interests in each individual case is required.[223] This can be summarised as follows in the words of the KG Berlin:[224]

> "In this respect, the seriousness of the breach of procedural law and the gravity of the alleged offence are of key significance. The seriousness of the breach of procedural law is determined particularly based on the degree of blame that can be placed on the person issuing the order or the person executing it, and based on the encroachment's impact on fundamental rights, as well as on whether the piece of evidence could have been obtained without a breach of law and whether the violated procedural rule primarily served to protect the suspect or other purposes. Regarding the alleged offence one must bear in mind that the interest in unrestricted investigation increases with the severity of the offence a person is suspected of."

Limits to the balancing of interests are not reached until "the defendant doesn't have adequate possibilities to exert an influence on the course and outcome of the proceedings, the minimum requirements as to reliable investigation of the truth are no longer met, or *admitting* [emphasis by the authors] the information as evidence would lead to a disproportionate encroachment" of the fundamental right concerned.[225]

> "Moreover, the admissibility of information obtained by violating legal provisions may not be affirmed where this would lead to encouraging the unlawful taking of evidence. A ban on the admission of evidence may hence be required particularly after serious, deliberate, or objectively arbitrary breaches of the law in which fundamental law-related safeguards have been intentionally or systematically disregarded."[226]

According to the established case law of the Federal Court of Justice concerning orders pursuant to Section 100a StPO, a ban on the admission of evidence exists at

---

222 BVerfG NJW 2012, 907 (910, para. 117).

223 BGH NJW 1999, 959 (961).

224 KG Berlin, decision of 16 February 2005, Az. (5) 1 Ss 406/04 (63/04), para. 6.

225 BVerfG NJW 2012, 907 (910, para. 117).

226 BVerfG NJW 2012, 907 (910, para. 117). Also comparable BVerfG NJW 2009, 3225 et seq.

least when essential objective prerequisites for ordering the interception measure – such as the suspicion of an offence pursuant to Section 100a Subsection 2 StPO – are not fulfilled.[227]

The Federal Court of Justice has more precisely specified the necessary balancing of interests by means of a "maxim of proportionality."[228] According to this, criminal offences of substantial significance can justify the use of otherwise illegal investigative measures, if other investigative means would be considerably less likely to succeed or establishing the facts would be substantially more difficult.[229] Thus, the maxim of proportionality does not entail a shift in the standards applied when assessing the consequences of the unlawful collection of evidence. Rather, the assessment of the (performance of the) measure itself changes, depending on the significance of the offence and the availability of other investigative means.

Furthermore, for the ban on the admission of evidence to apply, the Federal Court of Justice requires in certain cases that the defendant – provided he is represented by a criminal defence attorney – explicitly object to the admission of unlawfully collected evidence.[230] Failing to do so precludes the right to raise the issue of admissibility on appeal.[231] This so-called objection solution applies, in particular, to a *violation of formalities of suspect interrogations* or in cases of secret investigative measures, such as the *interception of telecommunication*.[232]

In addition to the maxim of proportionality and the objection solution, an attempt to compensate procedural violations is made by applying special standards for the evaluation of evidence as well as by taking them into consideration when determining the sentence.[233] In detail, the relationship between the various instruments is unresolved.[234]

---

227 BGH NStZ 2006, 402 (403); NStZ 2003, 499.

228 *Roxin/Schünemann*, StPO, Section 24, paras. 30, 41.

229 See BGH GrS NJW 1996, 2940 (2941), for the use of a so-called *Hörfalle* (listening in on telephone conversations which the police induces a third party to lead with the suspect) on the basis of the investigative general clause of criminal procedure in Sections 161, 163 StPO.

230 For instructive commentary on the whole issue, see *Eschelbach*, Beck-OK StPO, Section 257, paras. 20 et seqq.

231 According to the courts, such a preclusion already applies if the objection is not made immediately following the introduction of the evidence into the main hearing pursuant to Section 257 Subsection 2 StPO, see BGH NJW 1992, 1463 as well as OLG Celle, NStZ 2014, 118 et seq.

232 *Eschelbach*, Beck-OK StPO, Section 257, para. 21.

233 *Roxin/Schünemann*, StPO, Section 24, para. 30; *Eschelbach*, Beck-OK StPO, Section 257, para. 21.

234 *Ibid*.

b) Admissibility of evidence when conditions of collection remain unclear

Problems also arise when the conditions of the collection of evidence and hence its lawfulness remains unknown because the prosecution authorities don't provide the relevant information. This may be the case when software solutions which were developed at great expense (e.g., for source telecommunication surveillance) would otherwise have to be revealed, thereby possibly compromising other investigations.[235] The prosecution authorities' interests in secrecy regarding their investigative methods can be guarded by excluding the public from the main hearing based on an endangerment of the public order pursuant to Section 172 No. 1 of the Courts Constitution Act (*Gerichtsverfassungsgesetz*, GVG).[236] To the extent this is deemed insufficient by the prosecution authorities', and particularly the police force's point of view (which will likely be the case), there exists the possibility for the responsible minister of the interior – being the highest superior police authority – to issue a blocking order (so-called *Sperrerklärung*) pursuant to Section 96 Sentence 1 StPO.[237] This order must be based on the endangerment of the welfare of the Federal Republic or of one of the *Länder* (Section 96 Sentence 1 StPO). This also includes detriments regarding the state's obligation to avert danger and prosecute crimes.[238] In particular, blocking orders can apply to source code or records on program architecture and thus prevent a review.[239]

According to the Federal Court of Justice, the sentencing court may principally rely on the investigative procedure having been conducted in accordance with the law (although this most likely won't readily apply to evidence gathered in foreign countries, for instance, on the basis of a European Investigation Order).[240] If there is doubt regarding the investigation's lawfulness, then the existence of circumstances potentially leading to bans on the collection and admission of evidence must be examined in an open evidentiary proceeding *(Freibeweisverfahren)*.[241] When a (lawful) blocking order is issued, these efforts usually prove futile. In this

---

235 Regarding source telecommunication surveillance, see *Beuth*, Der neue Staatstrojaner des BKA ist fertig, Zeit Online from 15 August 2014, accessible at http://www.zeit. de/digital/datenschutz/2014-08/staatstrojaner-bka-onlinedurchsuchung-fertig

236 *Walther*, Beck-OK GVG, Section 172, para. 1; Section 133 Subsection 1 RiStBV.

237 Regarding the minister's competency, see BGH NJW 1981, 1052.

238 *Köhler*, in: Meyer-Goßner/Schmitt, Section 96, para. 7.

239 In principle, Section 96 StPO does not apply to police authorities when they act in pursuit of repressive objectives (see *Wohlers*, in: SK-StPO, Section 96, para. 9). In this respect, they are subject to the instructional powers of the public prosecution office to whom they are obliged to transmit records of all developing investigations, see Section 163 Subsection 2 StPO. However, Section 163 Subsection 2 StPO only applies to records accumulating in the course of the investigation, and not to documents pursuant to Section 96 StPO already generally available which also concern preventive police work.

240 BGH NStZ 2006, 402 (403).

241 BGH NJW 1961, 1979 (1980); BGH StV 2012, 3 (4).

case, the executive power's interests in maintaining secrecy work *in dubio pro reo* in criminal proceedings.[242] However, all this entails is that the court must resort to surrogates for the inaccessible primary pieces of evidence and take account of the finding's subsequent limitations by evaluating the evidence in a particularly cautious and critical manner.[243]

3. Use of data outside the original proceedings

The question to what extent data collected in criminal proceedings may be used for purposes other than those occasioning their collection requires a nuanced answer. One must differentiate between data collected in the framework of other repressive investigative measures and data collected in the course of measures outside of criminal proceedings (for the latter, see above I.A.4., as well as below b.).

a) Data from other criminal investigations

If the data were collected on the basis of repressive measures, it is crucial to distinguish between data pertaining to different offences in a *substantive* sense but belonging to the same offence in a *procedural* sense, and data pertaining to offences lacking a direct connection to the original proceeding.[244]

Only in the latter case one can speak of a transfer in the first place and must this transfer be based on a legal provision governing the rededication.[245] Pursuant to Section 474 Subsection 1 StPO, information from proceedings other than the original proceeding may in principle be used. This use is, however, subject to certain restrictions when the relevant data were obtained on the basis of a measure only admissible where specified criminal offences are suspected, Section 477 Subsection 2 StPO. Pursuant to this provision, data from other criminal proceedings may in principle only be used "for evidentiary purposes" without the consent of the person concerned if the measure could also have been ordered for the prosecution of the criminal offence at hand – applied to Section 100a StPO this means only con-

---

[242] BVerfG NStZ 2007, 274 (275).

[243] BGH NJW 1985, 1789 (1790). Thus the dictum that interests in maintaining secrecy work "in dubio" really amounts to nothing more than a confirmation of the (supposedly) self-evident. See also above a) for the three other forms of dealing with procedural errors during the collection of evidence.

[244] Note: Regarding the facts and circumstances constituting "an offence" ("an" as in *one* instead of multiple different offences), German jurisprudence works with two different concepts of "offence" depending on whether the substantive assessment of the offence(s) is concerned (offence in a substantive sense) or the assessment is made with regard to procedural issues (offence in a procedural sense). With a few exceptions, the two concepts usually coincide in their conclusions. For more, see *Schmitt*, in: Meyer-Goßner/Schmitt, Section 264, para. 6.

[245] *Wittig*, Beck-OK StPO, Section 474, paras. 1, 3.

cerning an offence pursuant to Section 100a Subsection 2 StPO and provided the remaining prerequisites for an order are fulfilled.

The restrictive wording "for evidentiary purposes" in Section 477 Subsection 2 Sentence 2 StPO leads to the question whether chance discoveries may be used at least as investigative clues in other criminal proceedings without consent and without the prerequisites for an order being fulfilled.[246] The matter appears not yet to have been explicitly addressed by existing case law. But with regard to the comparable provision of Section 161 Subsection 2 Sentence 1 StPO, prevailing opinion considers such use admissible.[247] However, Sections 100e Subsection 6,[248] 100i Subsection 2 Sentence 2,[249] 101a Subsections 4, 5[250] and 108 Subsections 2, 3 StPO[251] remain unaffected pursuant to Section 477 Subsection 2 Sentence 4 StPO. They take precedence as *leges speciales* regarding chance discoveries.

b) Data from preventive police law-based investigations

When personal data are collected on the basis of preventive (police) investigations, the principle of purpose limitation generally prohibits a subsequent rededication. However, Section 161 Subsection 2 StPO allows the public prosecution office to use such data for evidentiary purposes if an empowerment for a corresponding (not necessarily identical) measure principally exists in the StPO and if such a measure could have been ordered under the circumstances of the case in question ("hypothetical surrogate measure"). This also applies to cases in which the use of collected data for purposes of criminal prosecution is already envisaged.

---

246 See KK/*Grieg*, Section 477, para. 3.

247 BeckOK StPO/*Sackreuther*, 34. ed. 1.7.2019, StPO § 161 Rn. 15

248 Regulates the use of personal data gathered with the help of telecommunications surveillance, by means of an "online search" an through acoustic surveillance of private premises.

249 Prohibits further use of personal data from technical investigation measures concerning mobile terminal devices.

250 Subsection 4: Regulates the use of traffic data collected in the course of criminal proceedings.

Subsection 5: Regulates the use of traffic data collected in the course of police law investigations.

251 Subsection 2: Objects relating to the termination of a pregnancy which are found at the premise of a physician are inadmissible as evidence in respect of a criminal offence pursuant to Section 218 StPO.

Subsection 3: Limited admissibility of further use of objects covered by the right to refuse to testify accorded to certain bearers of professional secrets.

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

The exchange of intercepted electronic communication data between Germany and foreign countries is part of the scheme on mutual legal assistance in criminal matters (in the following: MLA). In German law, it is also called "other legal assistance" *(sonstige Rechtshilfe)*. Sometimes – in a narrower sense – the term "evidence gathering abroad" is used, too. According to Section 1 Subsection 3 of the Act on International Cooperation in Criminal Matters of 23 December 1982 (*Gesetz über die international Rechtshilfe in Strafsachen*, IRG – in the following: AICCM), provisions of international treaties shall take precedence before the provisions of this law to the extent that they have become directly applicable national law. In order to become directly applicable, the treaties must be enacted in the form of federal law (Article 59 Subsection 2 GG). Furthermore, the relevant treaty provision must be self-executing, i.e., it must be clear and sufficiently determined, and it must impose duties or rights for state organs or individuals without the need for further implementation by a national law.

Section 1 Subsection 4 AICCM stipulates that this Act shall govern the support in criminal proceedings involving a Member State of the European Union. This means that the German law implementing Union law on judicial cooperation, such as Framework Decisions or Directives, is embedded in the AICCM. The relationship between the implementing law and international treaties/conventions is regulated in the different parts of the AICCM relating to the specific form of international cooperation in criminal matters. Regarding "other legal assistance," Section 91 Subsection 2 AICCM stipulates that the German law implementing Union law that regulates mutual assistance matters, such as the Directive on the European Investigation Order, takes precedence over the international agreements mentioned in Section 1 Subsection 3 AICCM, insofar as it contains exhaustive regulations. This means that the rules of international MLA conventions or treaties may remain applicable if they facilitate legal cooperation in criminal matters. However, the stipulation cannot be interpreted as being a general rule that MLA can be provided on the most efficient and most favorable legal basis ("principle of the most favorable MLA rule" – *Grundsatz der Meistbegünstigung*). If a MLA request, e.g., a European Investigation Order, is declared inadmissible in accordance with the rules implementing the Union law, it cannot be circumvented by resorting to "more MLA-friendly" treaty provisions.[252] Since, however, the Union law and the national German implementation law already contain provisions that strengthen and facilitate MLA to the greatest possible extent in comparison to previous MLA agreements, the ques-

[252] *Wörner*, in: Ambos/König/Rackow (eds.), Rechtshilferecht in Strafsachen, HT 4, mn. 477 with further references.

tion as to the applicable law regarding the relationship between Union law and treaties on international cooperation in criminal matters is more or less theoretical.

Directive 2014/41/EU regarding the European Investigation Order in criminal matters was implemented into Part X, Section 2 of the AICCM (Sections 91a–91j).[253] Section 91 Subsection 1 AICCM and Section 91a Subsection 4 No. 1 AICCM clarify that the general provisions of the AICCM on mutual legal assistance apply unless there are specific provisions implementing the Union act in Part X of the AICCM.

Legal bases for cooperation regarding the interception and recording of telecommunications can therefore be:

– the provisions implementing the Directive on the European Investigation Order (among the EU Member States taking part in this scheme) – below 1;
– international conventions/agreements, which could be multilateral ones (below 2.) or bilateral ones (below 3.);
– the German legislation on mutual legal assistance in criminal matters (i.e., above all, the AICCM), if there neither the Directive on the European Investigation Order nor conventions/agreements apply (so-called non-treaty-based MLA – below 4.)

1. European Investigation Order and its implementation in Germany

Cross-border cooperation in the interception of telecommunications with EU Member States for which the rules of Directive 2014/41/EU regarding the European Investigation Order (in the following: Directive EIO) are binding (i.e., all EU Member States except Denmark and Ireland) follows the regulation of the German law implementing the Directive in Sections 91a et seqq. AICCM (see supra). It covers both EIO requests that are handled by the German judicial authorities (Germany as the executing state) and the outgoing requests of German authorities (Germany as the issuing state).

a) Implementation of the general provisions of the Directive EIO

In general, the Federal Government, which drafted the implementing law, does not see much difference between the Directive EIO and the conventional MLA

[253] The provisions transposing the Directive EIO into national law were introduced by supplementing and amending the Act on International Legal Assistance in Criminal Matters (*Gesetz über die internationale Rechtshilfe in Strafsachen* – IRG), see Federal Law Gazette (BGBl. I 2017, pp. 31 et seq.) The amendments to the AICCM entered into force on 22 May 2017.

scheme as regards the rules in substance. It does, however, consider the following points to be an added value of the EIO:[254]

– strengthened duties on the part of the authorities of the issuing and executing states to communicate with one another, so that better planning of criminal proceedings is possible;
– duty to carry out the investigative measure within certain time limits, which will accelerate MLA within the EU;
– use of standard forms which is considered ensuring better quality of MLA requests.[255]

As with the other EU instruments based on the principle of mutual recognition (e.g., European Arrest Warrant), the German legislator embedded the provisions of the Directive EIO into the existing law on international cooperation in criminal matters. This means, on the one hand, that the general provisions of the Directive, in particular the refusal and suspension grounds and the formal requirements on an EIO, were – more or less – taken over "one-to-one". Notwithstanding, well-established principles of the German law on international cooperation in criminal matters were maintained, in particular the competences of German authorities and the procedure of handling requests. Moreover, the terminology of the conventional system was not changed, e.g., the German legislator, for instance, preferred to further use "request" instead of "European Investigation Order" or "requested and requesting state" instead of "issuing and executing state." On the other hand, the delineation between the corpus implementing the Directive EIO (Part X, Section 2 AICCM) and other rules governing conventional mutual legal assistance is difficult; often, the rules implementing the Directive EIO include a number of clarifications in relation to the already existing provisions.

A main difference between the existing rules for conventional MLA and the new rules on the EIO is the distinction between grounds for the admissibility of a request *(Zulässigkeitsgründe)* and those for granting a request[256] *(Bewilligungsgründe)*. The implementing law highlights that the Directive EIO stipulates the grounds for refusal (reasons why a MLA request is admissible or approvable) in an exclusive way. Furthermore, it is acknowledged that the refusal grounds must be interpreted restrictively in the light of the principle of mutual recognition.[257] The legislator follows, however, the technique already chosen for the implementation of the Framework Decision on the European Arrest Warrant, i.e.:

---

[254] Cf. Press Release of 20 July 2016: https://www.bmjv.de/SharedDocs/Artikel/DE/2016/07202016_EU_Ermittlungsanordnung.html?cms_app=true

[255] For the interception of telecommunications, see particularly Section H7 of the form, Annex A of the Directive EIO, Official Journal EU 2014 L 130, p. 29.

[256] The term "approvability" is also used in this context.

[257] See also CJEU, 6.12.2018, C-551/18 PPPU ("*IK*").

– Some grounds for refusal (as listed in Article 11 Directive EIO) are seen as grounds of admissibility, i.e., these are compelling reasons to deny a request.[258] They apply, for instance, if there is an immunity or a privilege[259] or if there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with Germany's obligations in accordance with Article 6 TEU and the Charter of Fundamental Rights.[260]
– Others are implemented as grounds of approvability, i.e., the executing German authority has a discretion to perform a request, although the requirements of a refusal ground are, in principle, met.[261] For instance, the possibilities to refuse the execution for reasons of national security interests,[262] situations of *ne bis in idem*,[263] or jurisdiction for offences that have been committed outside the territory of the issuing state or entirely/partially on the German territory[264] are considered under this category of approvability.

In particular, this distinction entails effects on the judicial review.[265]

Another ground for refusal comes into play if it is not possible to make recourse to an investigative measure other than that indicated in the EIO where the alternative measure would achieve the same result. This applies where the investigative measure indicated in the EIO does not exist under German law or would not be available in a similar domestic case.[266]

The execution of an EIO request may also be refused if formal requirements are not met, e.g., if the form in annex A of the Directive EIO is not used or the EIO is not issued or validated by a judicial authority in the sense of Article 2 lit. c) Directive EIO.[267]

---

[258] See Section 91b AICCM.

[259] Section 91b Subsection 1 No. 2 AICCM implementing Article 11 para. 1 lit. a) Directive EIO.

[260] Section 91b Subsection 3 implementing Article 11 para. 1 lit. f) Directive EIO.

[261] See Section 91e AICCM.

[262] Section 91e Subsection 1 No. 1 AICCM implementing Article 11 para. 1 lit. b) Directive EIO.

[263] Section 91e Subsection 1 No. 2 AICCM implementing Article 11 para. 1 lit. d) Directive EIO.

[264] Section 91e Subsection 1 No. 3 AICCCM implementing Article 11 para. 1 lit. e) Directive EIO.

[265] Within the judicial review of Section 61 AICCM, the Higher Regional Court now also has to take a decision on the refusal grounds that concern the approvability of the request, i.e., it must decide on the correct use of the discretion as applied by the granting authority (cf. Section 91i Subsection 1 AICCM).

[266] Cf. Section 91f Subsection 5 in connection with Subsection 2 AICCM implementing Article 10 para. 1 Directive EIO. Section 91f entitled "Recourse to other investigative measures" also includes the obligation for German authorities to make recourse to a less intrusive measure which would achieve the same result as the investigative measure indicated in the EIO (Subsection 1 implementing Article 10 para. 3 Directive EIO).

[267] Cf. Section 91d AICCM. See in this context also the request for a preliminary ruling from the Landesgericht für Strafsachen Wien (Austria) lodged on 2 August 2019 – Crimi-

b) Implementation of the specific provision on the interception of telecommunications (Arts. 30 and 31 Directive EIO)

(1) Regarding the specific rules on the interception of telecommunications, which require the technical assistance of another Member State in Article 30 Directive EIO (and which are largely aligned with Article 18 MLA Convention EU, see infra), the German legislator principally saw no need for specific legal implementing provisions.[268] It refers to the already possible investigative measures on the surveillance of telecommunications, as described in No. 77a RiVASt (cf. infra 4.). This confirms that Germany is not only able to render MLA in the form of the interception of the content of telecommunications but also in the form of obtaining[269] telecommunications traffic data. However, in both cases, the respective requirements of the national criminal procedural law must be fulfilled (Sections 100a, 100d, 100e, 100g, and 101a GCPC).

In this context, the Section 91c Subsection 2 No. 2 lit. c) AICCM refers to the "special" grounds for refusal as stipulated in Article 30 Subsection 5 Directive EIO. According to this provision, and in addition to the grounds for non-execution referred to in Article 11 Directive EIO (that are implemented in Sections 91b and 91e AICCM, see supra a.), the execution of an EIO for the interception of telecommunications, for which the technical assistance of a Member State is needed, may also be refused where the investigative measure would not have been authorized in a similar domestic case.[270] The text stipulates that, in case of requests for the interception of telecommunications, MLA can be provided only if assistance

---

nal proceedings against A (Case C-584/19). Question referred: Are the terms 'judicial authority' within the meaning of Article 1(1) of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters and 'public prosecutor' within the meaning of Article 2(c)(i) of the aforementioned Directive to be interpreted as also including the public prosecutor's offices of a Member State which are exposed to the risk of being directly or indirectly subject to orders or individual instructions from the executive, such as the Senator of Justice in Hamburg, in the context of the adoption of a decision on the issuance of a European investigation order?

[268] Entwurf eines […] Gesetzes zur Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen (in the following: RegE EEA), BR-Drs. 421/16, also available at https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_EU_Ermittlungsanordnung.pdf;jsessionid=99E4C8B80707A8CF4263769E14B26535.1_cid324?__blob=publicationFile&v=3, pp. 45 et seq. In the following, the references made relate to the Internet document.

[269] The RegE EEA clarified that, for telecommunications traffic data already in the possession of the German authorities (historic data), Article 30 Directive EIO does not apply. However, the handing over of these traffic data is regarded a coercive measure, as a consequence of which Article 10 Subsection 2 Directive EIO also does not apply. Therefore, Articles 10 Subsection 1 and 11 Directive EIO remain fully applicable. The handing over of historic traffic data is only possible if no refusal ground or no recourse to a different type of measure is given (Section 66 AICCM and Sections 91b, 91e, 91f AICCM).

[270] Hence, this ground for refusal was transposed explicitly.

can be rendered to German courts and authorities under the conditions of Section 59 Subsection 3. Hence, the German legislator clarified that the Directive EIO will not entail a change compared to the current system, i.e., Section 59 Subsection 3 AICCM (cf. also infra) remains fully applicable for certain investigative measures that are requested on the basis of the Directive EIO.[271]

The explanatory report of the bill further points out that Article 30 Subsection 6 Directive EIO alters the system of Article 18 MLA Convention EU insofar as the immediate (real-time) transmission of telecommunications is no longer considered the rule. It is now up to the involved states to agree on whether the interception of telecommunications should be carried out in the form of immediate transmission or in the form of subsequent transmission of recorded telecommunications. Germany considered no need for implementation of this regulation in the Directive because German MLA law already allows for both possibilities and also assumes that the technical details of the interception are subject to individual agreements between the competent authorities of the requesting and requested states. The explanatory report indicates that the solution must be found on a case-by-case basis. It may be dependent on technical aspects, such as secure communication channels, as well as the presumably sufficient protection of the fundamental rights of the person concerned.[272]

Germany did also not implement Article 30 Subsection 7 Directive EIO, which foresees the possibility for the issuing state to request a transcription, decoding or decrypting of the recording subject to the agreement of the executing authority. Article 30 Subsection 7 largely corresponds to Article 18 Subsection 8 MLA Convention EU. Germany already assumes that the German authorities should comply with the formalities and procedures indicated by the requesting state unless they were to contradict contingent provisions of its national law (No. 22 Subsection 1 Sentence 2 RiVASt).

Regarding the special provision on the costs resulting from the application of Article 30 Directive EIO (Article 30 Subsection 8 Directive EIO), the German law already complied with the EU requirements (Section 75 AICCM). However, the clarifications are included in the RiVASt.

(2) In contrast, the German legislator considered certain amendments necessary in cases involving the interception of telecommunications pursuant to Article 31 Directive EIO in which no technical assistance from another Member State is needed. In particular, adaptations of the German law and the German guidelines were

---

[271] RegE EEA, *op. cit.* (fn. 261), p. 70. The clarification is considered particularly necessary because Section 59 Subsection 3 AICCM is modified by Article 10 para. 2 Directive EIO.

[272] RegE EEA, *op. cit.* (fn. 268), p. 47.

made as far as the differences between Article 31 Directive EIO and Article 20 MLA Convention EU are concerned.[273]

Section 91d AICCM stipulates the necessity to use the form in annex C of the Directive EIO, i.e., for all incoming notifications of an EU Member State about the interception of telecommunications that will be, is or has been carried out on the territory of Germany with its technical assistance. Subsection 91j AICCM orders the same for the reverse case of outgoing notifications.

Section 91g AICCM transposes the possibilities of Germany to react to cross-border interception of telecommunications without its technical assistance and the time limits as provided for in Article 31 Subsection 3 Directive EIO. Accordingly, German authorities are allowed to deny such requests where the investigative measure would not have been authorized in a similar domestic case. The German authorities must then inform the competent authorities of the issuing Member State without delay (but within 96 hours at the latest) after receipt of the notification. This information must include that (1) the interception cannot be carried out or must be terminated, and (2) that information which has already been collected during the stay of the person concerned on German territory cannot be used by the issuing state or used under conditions.

In addition, Section 92d AICCM includes a regulation that allows the rapid determination of the locally competent court that hast to decide on the admissibility of the incoming request of the surveillance of telecommunications without the technical assistance of German authorities. The RiVASt includes guidelines for the public prosecution offices how to handle notifications pursuant to Article 31 Directive EIO and their obligation to apply for a decision by the competent court.[274]

c) Notifications

In accordance with Article 33 Subsection 1 lit. a) and b) Directive EIO, Germany made the following notification:[275]

> "In Germany, the issuing or executing authority may be any judicial authority (in particular: the Federal Prosecutor General at the Federal Court of Justice, the local public prosecution offices, the prosecutors general of the Länder and the Central Office of the Land Justice Administrations for the Investigation of National Socialist Crimes in Ludwigsburg, or any court having jurisdiction in criminal matters), depending on the allocation of responsibilities in the relevant Land.

---

[273] Cf. in more detail RegE EEA, *op. cit.* (fn. 268), pp. 48 et seq.

[274] Nos. 202 and 212 RiVASt clarifying that Nr. 77a RiVASt para. 4 sentence 1 applies *mutatis mutandis*.

[275] See the letter of the Permanent Representation of the Federal Republic of Germany to the European Union in Brussels of 14 March 2017, Ref. Ares(2018)2144837 – 23/04/2018.

Administrative authorities responsible for prosecuting and punishing administrative offences under German law can also be issuing and executing authorities.

In compliance with Article 2(c) EIO Directive, requests from German administrative authorities to other EU Member States must usually be validated by the public prosecutor's office at the Regional Court (Landgericht) in whose district the administrative authority is based. By way of derogation, the Länder are free to assign jurisdiction for such validation to a court, or to regulate the local jurisdiction of the validating public prosecutor's office in other ways (Section 91j(2) IRG).

Requests from German revenue authorities which are independently conducting a criminal investigation pursuant to Section 386(2) Tax Code (*Abgabenordnung* – AO) do not require validation by a judicial authority or a court. In this case, the revenue authorities exercise the rights and responsibilities of a public prosecutor's office in accordance with Section 399(1) Tax Code in conjunction with Section 77(1) IRG and themselves act as a judicial authority within the meaning of Article 2(c) EIO Directive.

With reference to Article 5(2) EIO Directive, incoming requests to authorities in Germany on the basis of the EIO Directive must be in German."

2. International (multilateral) cooperation

As far as multilateral international agreements on mutual legal assistance applicable to the interception of electronic communications are concerned, the conventions/treaties that Germany ratified and applies are listed in the following section. A distinction should be made in this context between a first layer and a second layer. The first layer concerns whether the international MLA conventions or treaties are generally applicable to any criminal offense (a) or whether they regulate cooperation for a specific crime (b); the second layer concerns the various "legal areas" that must be distinguished, i.e., whether cooperation relates to contracting parties of the conventions/treaties established by the Council of Europe (European level), to Member States of the European Union or states associated to the EU (EU level), or to third countries (global and UN level).

a) Non-crime specific international MLA conventions

aa) European level (cooperation within the Council of Europe)

Germany ratified and applies the *European Convention on Mutual Assistance in Criminal Matters of 20 April 1959*.[276] It entered into force for Germany on 1 January 1977. According to the German understanding, the general clause of this Convention (Article 1) includes the obligation to provide legal assistance in case of a request on the interception of electronic communications. The reasoning behind this is that the 1959 Convention does not contain an exclusive listing of possible MLA measures. Under the German viewpoint, this is also confirmed by the Com-

[276] Since the 1959 Convention is a so-called "open" Convention, non-European parties can also be part of it. Therefore, cooperation on the basis of this Convention between Germany and, e.g., Chile, Israel, and South Korea is also possible.

mittee of Ministers' Recommendation Rec(85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications.[277] Therefore, Article 1 Subsection 1, Article 3 Subsection 1 of the 1959 Convention in connection with the Recommendation can form a relevant legal basis for rendering assistance in the interception of telecommunication in relation to countries being party to the Convention.[278] However, schemes that reinforce cooperation in this regard take precedence, such as the Directive EIO (supra 1.) or the 2000 EU MLA Convention (infra bb.).

Regarding the general prerequisites for MLA, the following declarations and reservations of Germany with regard to the 1959 Convention should be considered in the context of the interception of telecommunications:

- Regarding Article 5: Search and seizure of property is permitted only if the conditions of Article 5, paragraph 1.a and c of the European Convention on Mutual Assistance in Criminal Matters have been met.
- Regarding Article 16: Where the request for mutual assistance and the annexed documents are not in the German language they must be accompanied by translations of the request and the supporting documents into the German language or into one of the official languages of the Council of Europe.

Furthermore, Germany ratified the *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 17 March 1978*, which entered into force for Germany on 6 June 1991. Germany made the following reservations and declarations with respect to the 1978 Additional Protocol:

- Regarding Article 2 of the Additional Protocol, the Federal Republic of Germany, in accordance with Article 8(2)(a), reserves the right to make the execution of letters rogatory of any kind in proceedings concerning contraventions of regulations governing international transfer of capital and payments, dependent on the condition that the offence motivating the letters rogatory is punishable under German law as well, or would be so punishable after analogous conversion of the facts.
- Regarding Article 2 of the Additional Protocol, the Federal Republic of Germany, in accordance with Article 8(2)(a), reserves the right to make the execution of letters rogatory for search or seizure of property in respect of other fiscal offences dependent on the condition that the offence motivating the letters rogatory is punishable under German law as well, or would be so punishable after analogous conversion of the facts.

---

[277] Available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804e6b5e

[278] Since the 1959 CoE MLA Convention is an open agreement, this could also be non-European countries, e.g., Chile, Israel or the Republic of Korea that also ratified the Convention.

- Regarding Article 8 of the Additional Protocol, the Federal Republic of Germany proceeds on the understanding that under the scope of application of the Convention, as extended by the Additional Protocol, there is no obligation to render assistance in the event that the effort and expenses to be expected in executing the letters rogatory are disproportionate to the subject-matter and execution could thus prejudice essential German interests.

Germany also ratified the *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 8 November 2001*, which entered into force on 1 June 2015. The following reservations and declarations are worth noting:

- In accordance with Article 26 (5) of the Second Additional Protocol, the Federal Republic of Germany declares that, within the framework of procedures for which it could have refused or limited the transmission or the use of personal data in accordance with the provisions of the Convention or one of its Protocols, personal data transmitted to another Party may not be used by the other Party for the purposes of Article 26 (1) unless with the previous consent of the Federal Republic of Germany.
- In addition to [the above], the Federal Republic of Germany declares the following concerning the whole of Article 26 of the Second Additional Protocol: In applying this Article, it is the understanding of the Federal Republic of Germany that the Parties remain free, in consideration of the data protection interests of the persons concerned, to apply provisions that rule out the transmission of data to another Party or that allow transmission only subject to certain conditions. The Federal Republic of Germany therefore reserves the right, as necessary, to make the exchange of personal data dependent on compliance with the data protection requirements of the domestic law of the Federal Republic of Germany in specific individual cases. To this extent, the Federal Republic of Germany also reserves the right to make, in individual cases, mutual legal assistance on the basis of the Convention and its Protocols dependent on its limitation to a specific use or a special purpose. In this context, the Federal Republic of Germany makes reference to its declaration in respect of Article 12 (2) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981. According to this declaration, it is the understanding of the Federal Republic of Germany that Article 12 (2) of the Convention referred to above allows the Parties the freedom to make provisions in their national data protection law which may in certain cases, in consideration of the data protection interests of the persons concerned, rule out the transmission of data.
- Notwithstanding the above reservations and declarations, the Federal Republic of Germany declares in accordance with Article 33 (1) first and second sentences that it upholds all the reservations und declarations made in respect of the Convention and the Protocol […].

- In accordance with Article 4 (8) (b), the Federal Republic of Germany declares that requests, except urgent requests, are to be addressed to the Federal Office of Justice.
- In accordance with Article 4 (8) (d), the Federal Republic of Germany declares that requests by administrative authorities are always to be addressed to the Federal Office of Justice, i.e., also in urgent cases.
- In accordance with Article 6 of the Second Additional Protocol, the Federal Republic of Germany up-dates its declaration in respect of Article 24 of the Convention and defines what authorities it will, for the purpose of the Convention, deem judicial authorities. These are as follows:
  - *Bundesministerium der Justiz und für Verbraucherschutz* (Federal Ministry of Justice and Consumer Protection), Berlin
  - *Bundesamt für Justiz* (*Federal* Office of Justice), Bonn
  - *Bundesgerichtshof* (Federal Court of Justice), Karlsruhe
  - *Generalbundesanwalt beim Bundesgerichtshof* (Federal Prosecutor-General at the Federal Court of Justice), Karlsruhe
  - *Justizministerium Baden-Württemberg* (Ministry of Justice of Land Baden-Württemberg), Stuttgart
  - *Bayerische Staatsministerium der Justiz* (Bavarian Ministry of Justice), Munich
  - *Senatsverwaltung für Justiz und Verbraucherschutz* (Senate Department for Justice and Consumer Protection), Berlin
  - *Ministerium der Justiz und für Europa und Verbraucherschutz des Landes Brandenburg* (Ministry of Justice and for Europe and Consumer Protection of Land Brandenburg), Potsdam
  - *Senator für Justiz und Verfassung* (Senator of Justice and Constitution), Bremen
  - *Behörde für Justiz und Gleichstellung der Freien und Hansestadt Hamburg* (Free and Hanseatic City of Hamburg Ministry of Justice and Equalities)
  - *Hessische Ministerium der Justiz* (Hessian Ministry of Justice), Wiesbaden
  - *Justizministerium Mecklenburg-Vorpommern* (Ministry of Justice of Mecklenburg-Western Pomerania), Schwerin
  - *Niedersächsische Justizministerium* (Ministry of Justice of Lower Saxony), Hannover
  - *Justizministerium des Landes Nordrhein-Westfalen* (Ministry of Justice of North Rhine-Westphalia), Düsseldorf
  - *Ministerium der Justiz und für Verbraucherschutz des Landes Rheinland-Pfalz* (Ministry of Justice and Consumer Protection of the State of Rhineland-Palatinate), Mainz

- *Ministerium der Justiz des Saarlandes* (Ministry of Justice of Saarland), Saarbrücken
- *Sächsische Staatsministerium der Justiz* (Saxon State Ministry of Justice), Dresden
- *Ministerium für Justiz und Gleichstellung des Landes Sachsen-Anhalt* (Ministry of Justice and Gender Equality, Saxony-Anhalt), Magdeburg
- *Ministerium für Justiz, Kultur und Europa des Landes Schleswig-Holstein* (Ministry of Justice, Cultural and European Affairs Schleswig-Holstein), Kiel
- *Thüringer Ministerium für Justiz* (Thuringian Ministry of Justice), Erfurt
- *Oberlandesgerichte* (the higher regional courts)
- *Landgerichte* (the regional courts)
- *Amtsgerichte* (the local courts)
- *Generalstaatsanwaltschaften/die Staatsanwaltschaften bei den Oberlandesgerichten* (offices of the public prosecutors general)
- *Staatsanwaltschaften/Staatsanwaltschaften bei den Landgerichten* (public prosecution offices)
- *Zentrale Stelle der Landesjustizverwaltungen zur Aufklärung nationalsozialistischer Verbrechen* (Central Office of the Land Judicial Authorities for the Investigation of National Socialist Crimes), Ludwigsburg.

bb) EU level

Germany ratified the *Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union* (in the following MLA Convention EU) as well as its additional *Protocol to the Convention of 16 October 2001 on Mutual Assistance in Criminal Matters between the Member States of the European Union* (in the following: MLA Protocol EU). Both MLA Convention EU and MLA Protocol EU entered into force for Germany on 2 February 2006.[279] In relation to the specific rules on the interception of telecommunications, the Federal Republic of Germany declared with reference to Article 24(1)(e) of the MLA Convention EU "that the competent contact point in accordance with Article 20(4)(d) is the following: Bundeskriminalamt 65173 Wiesbaden Phone: 0049 (0) 611-55-13101 Fax: 0049 (0) 611-55-12141 e-Mail: mail@bka.bund.de."

Germany did not make declarations concerning the MLA Protocol EU.

The EU Convention does no longer apply to mutual legal assistance in the interception of telecommunications with EU countries that are bound by the Directive

[279] Cf. https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_RatificationsByCou.aspx and http://www.consilium.europa.eu/en/documents-publications/agreements-conventions/agreement/?aid=2001090

2014/41/EU regarding the European Investigation Order in criminal matters (Article 34 Subsection 1 lit. c) Directive EIO). These MLA requests are performed in accordance with the rules of the German law implementing the Directive (see supra 1.).

The MLA Convention EU (and in particular its Articles 17 et seqq.) will, however, further be the legal basis for the interception of telecommunications in the following cases:

– in relation to EU Member States that are not bound by the Directive EIO, but ratified the Convention (currently: Denmark);
– in relation to Iceland and Norway through the references in Article 2 Subsection 1 MLA Convention EU and Article 1 of the Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the application of certain provisions of the Convention of 29 may 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and the 2001 Protocol thereto;[280]
– mutual legal assistance requests received before 22 May 2017 by EU Member States bound to the Directive and party of the MLA Convention EU.[281]

In relation to Ireland the 1959 Convention and its first and second protocol apply, because Ireland is neither bound by the Directive EIO nor has it ratified the MLA Convention EU.[282]

cc) Global level

There is currently no general worldwide international convention on mutual legal assistance in criminal matters. Cooperation with non-European countries[283] not relating to a specific area of crime (cf. b.) is either based on bilateral treaties (in particular with the United States[284] and Canada[285]) or on the national German law

---

[280] Official Journal EU 2004 L 26, p. 3.

[281] Cf. Article 35 para. 1 Directive EIO.

[282] The status of ratification of CoE conventions can be checked at the Treaty Office on https://www.coe.int/en/web/conventions/; the status of the EU Convention can be checked through the judicial library of the EJN at: https://www.ejn-crimjust.europa.eu/ejn/libcategories/EN/32/-1/-1/-1

[283] Except countries that ratified the European Convention on Mutual Legal Assistance of 1959 and/or its Protocols (cf. above).

[284] Cf. in particular Article 12 No. 1 of the Treaty of 14 October 2003 between the Federal Republic of Germany and the United States of America on Mutual Legal Assistance in Criminal Matters (MLA Treaty Germany-USA), according to which "[e]ach Party may at the request of the other Party, within its possibilities and under the conditions prescribed by its domestic law, take the necessary steps for the surveillance of telecommunications."

[285] Cf. Treaty of 13 May 2002 between Canada and the Federal Republic of Germany on Mutual Assistance in Criminal Matters (MLA Treaty Germany-Canada). The Treaty does not contain a specific provision on the surveillance of telecommunications. However,

on international cooperation in criminal matters (non-treaty-based MLA – cf. 4. below).

b) Conventions regulating cooperation for a specific area of crime

Regarding the relevant international conventions that contain obligations on MLA for a specific area of crime, the following should be noted:

aa) Global level

On the global level, Germany ratified the *United Nations Convention against Transnational Organized Crime* of 15 November 2000. It entered into force for Germany on 14 June 2006. On the same date, the two additional protocols entered into force for Germany: (i) *The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime and the Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime*. Germany has not yet ratified the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime.[286]

bb) European level

Regarding the regional, European level, emphasis is placed on the ratification of the *Convention on Cybercrime of the Council of Europe* of 23 November 2001. It entered into force for Germany on 1 July 2009. Germany also ratified the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems of 28 January 2003. It entered into force for Germany on 1 October 2011.

3. Bilateral treaties

As regards the "European level," Germany concluded bilateral treaties on MLA that supplement the 1959 European Convention on Mutual Assistance in Criminal

---

Article 1 para. 5 lit. h) contains a general clause according to which assistance shall include "other assistance consistent with the objects of this Treaty, which is not inconsistent with the law of the Requested State." This clause includes the possibility – provided that the further requirements of the Treaty, in particular the double criminality requirement, are met – to execute requests on the interception of telecommunications (see BT-Drs. 15/2598, p. 18).

[286] For the status of ratification of the Convention and its protocols, consult the following website https://www.unodc.org/unodc/en/treaties/CTOC/signatures.html

Matters. These treaties aim at further developing the founding European Convention and thus facilitating and strengthening MLA with the corresponding countries. Such bilateral treaties were concluded with Austria (1972), France (1974), Israel (1977), Italy (1979), The Netherlands (1979), Switzerland (1969), the Czech Republic, and Poland. However, only the "more recent" bilateral supplementary treaties with the Czech Republic (2000) and Poland (2003) contain specific provisions on the interception of electronic communications.[287]

The question arises whether bilateral treaties in relation to EU Member States still apply after the Directive EIO came into force. The German government affirmed this question in its notification to Article 34(4) of the Directive EIO.[288] According to the author's view, this declaration is not in line with the wording and intention of Article 34 Directive EIO. The general reference to the bilateral treaties is too far-reaching. Applicability is only possible if the Directive EIO does not have "corresponding provisions" which is not the case in relation to the interception of telecommunications. Hence of practical importance are only the bilateral agreements with non-EU countries, i.e., Israel and Switzerland. As mentioned, these agreements do not include specific provisions on the interception of telecommunications, but the treaties' provisions are relevant for the general conditions to render MLA.

4. National regulation

The execution of requests relating to the interception/surveillance/recording of telecommunications that stem from countries with which Germany has no treaty-based relations is possible. However, the German granting authorities have a wide discretion to refuse a request because of foreign policy reasons.[289] In this case, the Act on International Cooperation in Criminal Matters (AICCM – *Internationales Rechtshilfegesetz*, IRG) applies. Although the AICCM does not contain specific provisions on the interception or surveillance of telecommunications, the execution of a respective request can be based on the general clause of Section 59 AICCM. It reads as follows:

> (1) At the request of a competent authority of a foreign State, other legal assistance in a criminal matter may be provided.
>
> (2) Legal assistance within the meaning of subsection (1) above shall be any kind of support given for foreign criminal proceedings regardless of whether the foreign pro-

---

287 The relevant provisions of the treaties (Article 17 in the treaty with the Czech Republic, and Article 16 in the treaty with Poland) are explained in detail at *Wahl*, Exchange of Intercepted Electronic Communication Data between Foreign Countries, in: Sieber/von zur Mühlen (eds.), Access to Telecommunication Data in Criminal Justice, 2016, pp. 578–579.

288 See the notification, *op. cit.* (n. 275).

289 Cf. *Schomburg/Lagodny*, Internationale Rechtshilfe in Strafsachen, 6th ed. 2020, Einleitung, mn. 34 with further references.

ceedings are conducted by a court or by an executive authority and whether the legal assistance is to be provided by a court or by an executive authority.

(3) Legal assistance may be provided only in those cases in which German courts and executive authorities could render mutual legal assistance to each other.

In the concrete case of a request from a foreign country that seeks the interception of telecommunications, the requirements of the respective provisions of the German Criminal Procedure Code (in the following: GCPC) must be met (Section 77 AICCM in connection with Sections 100a et seqq. GCPC).

An important national regulation concerning the interception of telecommunications is contained in No. 77a of the Guidelines on Relations with Foreign Countries in Criminal Law Matters (*Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten* – in the following: RiVASt).[290] The Guidelines were established by the Federal Government with the consent of the governments of the *Länder*. They are addressed to the courts, the prosecution services, and other executive authorities that deal with international cooperation in criminal matters and must be observed by them. Only if the judiciary takes decisions in its capacity as independent judges are the Guidelines not binding for them.[291]

No. 77a Subsection 1 RiVASt first confirms that the execution of requests on the interception of telecommunications in Germany is possible on the basis of both an international treaty/convention/agreement or on the basis of Section 59 Subsection 1 AICCM (non-treaty-based cooperation). Furthermore, No. 77a RiVASt confirms that the interception of the content of telecommunications is admissible only if it complies with the provisions of "Sections 100a, 100b, 101 GCPC."[292]

On the other hand, No. 77a contains important indications on the necessary assurances that must be provided for by the foreign country. It stipulates that – if not stated otherwise in an international agreement or if conditions as set in the context of handing over the records are not sufficient – the foreign authority must assure that

a) the requirements of the interception would be met, if such measure were carried out on the territory of the requesting state,
b) the obtained data are only used for the investigation and prosecution of the offense(s) to which the request relates to,
c) the recordings of the interception are destroyed when they are no longer needed for the criminal prosecution.

---

[290] The most recent version dates from 23 December 2016. The RiVASt is available (in German only) via the following link http://www.bmjv.de/SiteGlobals/Forms/Suche/RiVaStsuche_Formular.html?nn=6428404&templateQueryString=Suchbegriff

[291] No. 1 RiVASt.

[292] The current version of the RiVASt has not taken into account the recent reforms of the GCPC. The reference must therefore be read as: "Sections 100a, 100d, 100e, 101 GCPC."

In addition, No. 77a RiVASt deals with the issue of notification. The foreign authority must be informed that the German public prosecution office has to notify the participants in the telecommunication under surveillance of the surveillance measure pursuant to Section 101 GCPC if the surveillance measure is terminated and a notification is possible without jeopardizing the purpose of investigation, public security, or a person's life and limb. If the requesting state does not react within a specific time period (as set by the German authorities) or does not provide material facts that justify not making a notification, Germany assumes that the notification can be carried out.

No. 77a Subsection 2 RiVASt acknowledges that, under the conditions of Section 59 AICCM, German authorities can also provide a summary of the findings of a telecommunication interception, carried out for the purposes of a German criminal investigation, if this information is requested by the foreign state for the same offense or an offense that is listed in Section 100a GCPC (Sections 77 AICCM, 477 Subsection 2 Sentence 2 GCPC). Under the same conditions, copies of surveillance protocols, comprehensive notes on the content of the conversation, or recording tapes can be handed over.

No. 77a Subsection 3 RiVASt acknowledges that mutual legal assistance to a foreign authority can also be provided for information on telecommunication connections (Section 100g GCPC) if the requirements of Section 66 AICCM are met.[293] Regarding the obligation of the German authorities to notify "pursuant to Section 101 GCPC,"[294] the aforementioned rules apply *mutatis mutandis*.

No. 77a Subsection 4 contains procedural rules if a German authority is contacted within the framework of Article 20 Subsections 2 and 3 of the 2000 MLA Convention EU (interception of telecommunications without the need for technical assistance of another Member State).

---

[293] Section 66 AICCM deals with the handing over of objects. In particular, the requirements of Section 66 Subsection 2 AICCM must be given. Accordingly, surrender shall not be admissible unless

1. the offence on which the request is based contains elements of the *actus reus* and *mens rea* of a criminal offence or of an offence permitting the imposition of a fine under German law or unless mutatis mutandis it would be such an offence under German law,

2. an order for seizure by a competent authority of the requesting State is submitted or a declaration of such an authority shows that the requirements for seizure would exist if the objects were located in the requesting State, and

3. measures are in place to ensure that the rights of third parties will not be infringed and that objects handed over under a condition will be returned upon request without undue delay.

[294] Now: Section 101a (Subsection 6) GCPC.

B. Requirements and Procedure (Including the Handling of Privileged Information)

1. Incoming requests

a) Regular procedure

As regards incoming requests, it is first worth mentioning that Germany distinguishes between two procedures that are fundamental to German mutual legal assistance law and are particularly relevant for the area of "other assistance." The first procedure concerns the question of whether the assistance requested can be provided to the foreign state or requested from it, i.e., *whether* the conditions for mutual legal assistance are fulfilled and the request can be granted (procedure of approval – *Bewilligungsverfahren*). These conditions are mainly stipulated in the applicable international conventions and/or in the AICCM, respectively.

The second procedure deals with the question of the conditions and (coercive) measures that must be applied in order to enforce the request in domestic territory (enforcement procedure – *Vornahmeverfahren*). In this context, Section 59 Subsection 3 AICCM provides that legal assistance may be provided only under circumstances under which German courts and governmental authorities could render legal assistance to each other (cf. above). The question of *how* a request must be carried out is mainly a question of German procedural criminal law.[295] The procedure of granting a request is principally carried out prior to the procedure of enforcing the request. Both procedures are interconnected insofar as the request is not enforced if assistance cannot be provided, or assistance is not provided if the requested measure is not possible or illegal under German national law.[296]

Corresponding to the distinction between these two procedures, different authorities may also be involved in managing the request. Let us first look at the authorities who decide *whether* assistance can be provided. As a general rule, it is the Federation *(Bund)* which has jurisdiction over international legal assistance in criminal matters. In principle, the Federal Minister of Justice *(Bundesminister der Justiz)*, in consent with the Federal Foreign Office *(Auswärtiges Amt)*, decides on foreign requests and requests addressed to foreign states (Article 74 Subsection 1 AICCM). In 2007, the competence of the Federal Ministry of Justice was transferred to the Federal Office of Justice *(Bundesamt für Justiz)*, a subordinate authority of the Ministry, located in Bonn, and responsible, *inter alia*, for dealing with international cooperation in criminal matters on the federal level.[297]

---

[295] For the distinction, see *Trautmann/Zimmermann*, in: Schomburg/Lagodny, Internationale Rechtshilfe in Strafsachen, 6th ed., vor § 59, mn. 18 *et seq.*

[296] *Ahlbrecht*, in: Ahlbrecht/Böhm/Esser/Hugger/Kirsch/Rosenthal, Internationales Strafrecht in der Praxis, mn. 1006.

[297] Section 2 Subsection 2 No. 3 of the Act establishing the Federal Office of Justice *(Gesetz über die Errichtung des Bundesamts für Justiz)* in connection with the Decree of

However, the federation delegated its competences to the governments of the federal states *(Länder)* by the Agreement of Competences of 28 April 2004 *(Zuständigkeitsvereinbarung 2004)*.[298] The federal states in turn further transferred the competences by individual decrees, which vary from federal state to federal state. As a general rule, the (heads of the) prosecutors' offices at the Regional Courts *(Staatsanwaltschaften bei den Landgerichten)* are competent to decide on whether a request from an EU Member State can be granted. Some decrees of federal states stipulate that the competence of the prosecutors' offices is given only if an international agreement allows for the direct transmission of MLA requests. This is the case when the Directive EIO or the MLA Convention EU applies.[299] If the latter is not the case, the granting authority is the ministry of justice of the *Land* competent in the concrete case.

It is of note that the delegation to the prosecutors' offices does not mean that the federation loses its competence. The federal government (Federal Minister of Justice and Federal Office of Justice, respectively) remains legally responsible for issuing and executing requests for international legal assistance. It remains the "master" of the granting procedure and always has the possibility to appropriate a case. The judicial authorities of the federal states do not replace the competences of the federal government but act in its stead.

In general, it is important to note that international legal assistance, even if it is based on the EU instruments implementing the principle of mutual recognition in criminal matters (such as Directive EIO), is seen as a matter of foreign relations, which, according to constitutional law, lies within the competence of the Federation. The principal competence of the federal authorities is accompanied by certain reporting duties. If the request has "political, de facto, or legal importance" the federal state must act "in accordance with" the federal government (i.e., Federal Office of Justice).[300] Accordingly, the Guidelines on Relations with Foreign Countries in Criminal Law Matters (RiVASt) and the individual decrees of the *Länder* foresee a corresponding reporting duty of the competent prosecutor's office in these cases.[301] It is further stipulated by the 2004 Agreement of Competences that the granting

---

the Federal Ministry of Justice *(Erlass des Bundesministeriums der Justiz)* of 2 January 2007 – II B 6 – BfJ –, both published at *Schomburg/Lagodny*, Internationale Rechtshilfe in Strafsachen, 6th ed. 2020, Annex 1.

[298] Published at *Schomburg/Lagodny*, *ibid*., Annex 2.

[299] Germany did not make a declaration that a central authority would be competent to receive certain MLA requests (no declaration in this respect in accordance with Article 25 MLA Convention EU).

[300] No. 8 of the Agreement of Competences of 28 April 2004. In such important cases, the Federal Office of Justice itself will regularly inform the Federal Minstry of Justice. It may also enquire a statement by the Federal Ministry of Justice in order to receive guidance.

[301] Cf. No. 13 RiVASt.

authority "take into account the concerns of the federal government" in the above-mentioned significant cases.

The granting authority examines the request as to whether there is an obligation to render MLA to the foreign (requesting) state, i.e., whether the requirements of an international MLA agreement are met. If the answer is in the affirmative, the second stage of the procedure, the enforcement procedure, starts.

The authority which *enforces* the request ("how" of providing MLA) is the authority that would enforce the measure in purely domestic cases.[302] In a conventional criminal prosecution case of interception of telecommunications, the prosecutors' offices at the Regional Courts *(Staatsanwaltschaften bei den Landgerichten)* are competent to prepare the enforcement of the request.[303] As a result, the authority that normally grants the request and executes it by means of national law is identical (prosecutors' offices at the Regional Courts). The prosecutor must apply for an interception/surveillance order before the investigative judge at the local court *(Ermittlungsrichter beim Amtsgericht)*.[304]

One of the particularities of the German procedure is that the investigative judge is not only obliged to examine whether the requested coercive measure complies with national German criminal procedure ("how" – enforcement procedure) but also whether the requirements for rendering MLA are met. That means the judge also examines *whether* the MLA request is admissible under the conditions of the international treaty, e.g., whether the formal criteria as stipulated by the treaty are met or whether grounds for refusal (double criminality, proportionality, *ordre public*, etc.) are given, so that international assistance can be rendered or not.[305] If the

---

[302] *Trautmann/Zimmermann*, in: Schomburg/Lagodny, Internationale Rechtshilfe in Strafsachen, 6th. ed., vor § 59, mn. 23.

[303] I.e., if a not very serious crime (such as offences against the security of the state, terrorism, or crimes against international law) is at issue, which – pursuant to Section 120 Courts Constitution Act (*Gerichtsverfassungsgesetz*, GVG) – establishes the special competence of the Federal Prosecutor General *(Generalbundesanwalt)* or of the public prosecution office at the Higher Regional Court (*Staatsanwaltschaften bei den Oberlandesgerichten*, also called *Generalstaatsanwaltschaften*). Whether the Federal Prosecutor General or the public prosecution office at the Higher Regional Court is responsible is subject to rather complicated rules. As a rule, the Federal Prosecutor General accroaches competence when a criminal act as listed in Section 120 Courts Constitution Act is deemed to be of special significance.

[304] Section 162 GCPC. In case of responsibility on the part of the Federal Prosecutor General, the competent judge is the investigative judge at the Federal Court of Justice *(Ermittlungsrichter beim Bundesgerichtshof)*. If the crime at issue falls within the responsibility of the public prosecution office at the Higher Regional Court, the investigative judge at the Higher Regional Court is competent to decide on an interception order.

[305] In case of non-treaty-based cooperation, the requirement of the AICCM must be fulfilled. However, it does not differ substantially from the international MLA agreements that Germany applies (cf. also No. 77a RiVASt for the specific case of interception of telecommunications).

investigative judge at the local court considers the requirements for providing legal assistance not met, he/she must give reasons for his/her opinion and request a ruling by the Higher Regional Court *(Oberlandesgericht)*.[306]

The Higher Regional Court is also competent after an application by public prosecution service at the Higher Regional Court *(Generalstaatsanwaltschaft)*.[307] The Higher Regional Court decides on the admissibility of the request, i.e., whether legal assistance can be rendered. This corresponds to the German system that all questions relating to the admissibility of MLA are concentrated at the Higher Regional Court.

In sum, one can say that the Higher Regional Court decides on the admissibility of a MLA request by way of a preliminary ruling if (and only if) the investigative judge or the public prosecution service at the Higher Regional Court has doubts on the requirements of whether MLA can be rendered in accordance with the international agreements. The judgment of the Higher Regional Court regarding the admissibility of the MLA request is binding for the investigative judge at the local court and the enforcing authority.

The investigative judge at the local court, by contrast, always maintains its jurisdiction when it comes to the enforcement of the measure, which has to be assessed by German criminal procedural law.[308]

The prosecution service at the Regional Court *(Staatsanwaltschaften)*, which is primarily responsible for the incoming MLA request, has no right to apply for a preliminary ruling at the Higher Regional Court. However, it can recommend a respective application with its superior judicial authority, the prosecution service at the Higher Regional Court.

The Higher Regional Court itself can apply for a preliminary ruling on legal issues by the Federal Court of Justice *(Bundesgerichtshof)*. The Higher Regional Court shall request the decision of the Federal Court of Justice concerning a legal issue by means of a reasoned decision, if it deems a ruling by the Federal Court of Justice necessary for the clarification of a legal issue of fundamental significance or if it wishes to deviate from a decision of the Federal Court of Justice or from a decision taken after the coming into force of the AICCM by another Higher Regional Court concerning a legal issue (Section 61 Subsection 1 in connection with Section 42 Subsection 1 AICCM). Also the Federal Prosecutor General or the public prosecution service at the Higher Regional Court can make such a request to the Federal Court of Justice for the clarification of a legal issue.[309] Neither the investi-

---

306 Article 61 Subsection 1 Sentence 1 AICCM.

307 Article 61 Subsection 1 Sentence 2 AICCM.

308 Cf. *Trautmann/Zimmermann*, in: Schomburg/Lagodny, Internationale Rechtshilfe in Strafsachen, vor § 59, mn. 30.

309 Section 61 Subsection 1 in connection with Section 42 Subsection 2 AICCM.

gating judge nor the public prosecution service at the Regional Court or the person concerned have rights to make such a request.

b) Particularities in EIO procedures

The integration of the Directive EIO into the German system of international cooperation in criminal matters has, in principle, no consequences for the procedure described under a). In particular, the implementation does not touch upon the existing competences and the institutions involved in MLA. Furthermore, the two-step procedure – *Bewilligungs- und Vornahmeverfahren* – remains. Although the authority to grant a request was "delegated down" to the prosecution offices, the federal government remains "the master" of this part of the cooperation procedure that entails mainly the above-mentioned reporting obligations.

Complications occur in the procedure because of the implementation of the various refusal and suspension grounds as provided for in the Directive. The question first arises whether a provision is regulating "whether" assistance can be granted or "how" the request is enforced. The mandatory and facultative refusal grounds in Sections 91b and 91e AICCM as well as a rejection because of formal reasons (Section 91d) belong to the first category and are addressed to the granting authority, whereas the specific admissibility grounds for the surveillance of telecommunications in Section 91c and the replacement / refusal possibilities in Section 91f AICCM concern the second category.[310] Therefore, the latter is addressed to the authority enforcing the measure, i.e., regularly the investigating judge at the local court or – in exigent circumstances – the public prosecutor.[311]

The investigating judge who orders an interception of telecommunication must also examine whether one of the grounds of the first category apply and render assistance impossible. This examination does not only include the mandatory refusal grounds in Section 91b or the formal correctness of the request (Section 91d), but also the facultative refusal grounds as stipulated in Section 91e. Therefore, the granting authority, i.e., regularly the (head of the) public prosecution office must also justify how it applied the discretion conferred by the law. If the judge at the local court has doubts whether assistance can be rendered, i.e., one of the refusal grounds in Sections 91b, 91d, or 91e AICCM apply, he/she must request the decision of the Higher Regional Court.[312] As in conventional cases of mutual legal as-

---

[310] See details under A.1.a.

[311] Section 91h Subsection 1 AICCM implicitly clarifies that the EIO cannot circumvent the necessity of court authorisations in Germany where provided by its law (see also Article 2 lit. d) Sentence 2 Directive EIO). This is particularly relevant for the interception orders in the area of telecommunication surveillance (cf. Sections 100e, 101a GCPC).

[312] According to the Higher Regional Court of Frankfurt a.M., the request is inadmissible if the referring judge has doubts on the formal correctness of the request, but did not use the consultation procedure pursuant to Section 91d Subsection 3 AICCM beforehand

sistance, the prosecution service at the Higher Regional Court *(Generalstaatsanwaltschaft)* can also file such request.

According to Section 91i Subsection 1 AICCM, the Higher Regional Court can, on application, also verify the discretionary decisions during the EIO examination, i.e., the assessment whether legal assistance is rendered despite a facultative refusal ground or a ground for suspension as regulated in Section 91e Subsections 1–2 or although recourse to other investigative measures could have been made (Section 91f). In the situations of Section 91e, however, the Higher Regional Court can only verify errors of assessment *(Ermessensfehler)*, whereas the decision to make recourse to other, e.g., less invasive, investigative measures pursuant to Section 91f is fully verifiable.[313]

The wording of Section 91i Subsection 1 AICCM implies that the power of the Higher Regional Court to examine the discretionary decisions is not *proprio motu* and is of accessory nature. This means that the referring court or prosecution service at the Higher Regional Court must at least put forward a compelling ground for non-admissibility, such as those stipulated in Section 91b AICCM, and the must additionally request for examinations of the applied discretion or of the (potentially not used) alternative measures. It remains to the case law how applications are treated that only refer to an examination of assessment or only treat the question of alternative measures.

c) The rights of the individual for judicial review

The German law does not explicitly regulate how and to what extent an individual can proceed against any decisions to provide and to order MLA for the interception of telecommunications.[314] In other words, it has not been clarified which remedy applies in the two different stages of the MLA procedure (stage of the admissibility of the MLA request and stage of enforcement – cf. supra). In case of "open" coercive measures, such as search and seizure or the hearing of witnesses, the Federal Constitutional Court *(Bundesverfassungsgericht)* established the rule that the person concerned can seek legal remedies against the decision to order the investigative measure, i.e., to enforce the MLA (enforcement procedure). As part of this remedy, the person concerned can also claim that the competent court assesses

---

giving the the issuing authority the opportunity to remedy the errors (OLG Frankfurt a.M., Beschluss vom 2.10.2018 – 2 Ws 75/18 = NStZ-RR 2019, 62).

313 This implies the wording of Section 91i Subsection 1 Sentence 2 AICCM. See also *Brahms/Gut*, NStZ 2017, 388 (394). Indeed, it is questionable which cases under Section 91f can be referred since the decision to make recourse to alternative measures is already made by the "enforcing authority," including the investigative judge at the local court.

314 Section 61 AICCM only regulates the case of an application by a person claiming that his/her rights would be infringed if the return of an asset were ordered. This rule is not applied *mutatis mutandis* to other investigative/coercive measures at issue for rendering MLA.

the admissibility of the MLA request, i.e., whether the request complies with the requirements of the international treaty or, in case of non-treaty-based MLA, with the national MLA regulations (cf. A.1.–3. supra).[315] Thus, the remedy against the admissibility of the MLA request is integrated into the remedy against the ordering of the coercive measure, which follows the regular rules of the GCPC (so-called *Integrationslösung*).[316]

These rules must also apply accordingly in cases of the use of modern investigation techniques that are typically covert coercive measures, such as the interception of telecommunications. In these cases, the person concerned can regularly only seek subsequent legal protection *(nachträglicher Rechtsschutz)*, i.e., he/she can apply for a legal review of the lawfulness as well as the manner and means of implementation of the interception of telecommunications[317] *after* the measure was granted, ordered, and enforced. In this context, the above-mentioned notification of the person concerned (cf. A.3.) is important to secure his/her rights of judicial review. The person concerned can proceed against the decision ordering the interception of telecommunications within two weeks after notification of the interception measure against him/her (Section 77 AICCM in connection with Section 101 Subsection 7 Sentence 2 GCPC). In conventional cases,[318] the competent court for this judicial review is the investigative judge at the local court where the competent prosecution service is located (Section 77 AICCM in connection with Section 101 Subsection 7 Sentence 1, 162 Subsection 1 Sentence 1 GCPC).

The person concerned has no direct access to the Higher Regional Court in order to apply for a review of the admissibility of the MLA request. He/she is only able to ask the judge at the local court to apply for preliminary ruling at the Higher Regional Court as described above. If the Higher Regional Court takes a decision in the preliminary ruling procedure, its decision is final. There are no further ordinary remedies, such as a remedy to the Federal Court of Justice. However, the person concerned may file – as an extraordinary remedy – a constitutional complaint before the Federal Constitutional Court. In this case, the person concerned must substantiate that one of his/her fundamental rights as enshrined in the Basic Law was infringed by the decision of the Higher Regional Court or that the law on which the decision is based is unconstitutional.

German law does not contain provisions about the impact of the legal remedy on the use of evidence. In particular, interceptions of telecommunications result in a quick – in case of real-time surveillance even simultaneous – transfer of the evidentiary material to the requesting state before / without the knowledge of the person concerned. In order to render the legal remedy initiated by the individual effective,

---

315 BVerfG, EzSt IRG § 61 Nr. 2; BVerfG, decision of 24 June 1997 – 2 BvR 1581/95.

316 Cf. OLG Dresden, NStZ-RR 2011, 146.

317 Section 101 Subsection 7 GCPC.

318 Cf. supra V.B.1.b.

Swiss practitioners developed the model that the requested state should restrict the use of the transferred material and request from the requesting state that it can not be used *as evidence* in the criminal proceedings (e.g., in an indictment or in a court procedure deciding on the charge) as long as a final court decision has not been taken on the individual's complaint or as long as the individual has still the possibilities to exercise his right to judicial review in the requested state.[319] The requesting state should assure this restriction by a "warranty statement" *(Garantieerklärung)*. The authors suggest that the intercepted material can, however, be used for the purpose of searching the person concerned or co-perpetrators and for other investigative purposes *(Fahndungs- und Ermittlungszwecke)*.[320] These purposes could include, for instance, the use of the material to justify pre-trial detention or to follow other traces proving that a person has committed a criminal act. I recommend using this model also in Germany because it rightly balances the interest in an efficient procedure of prosecuting crime and the individual's interest in an effective remedy.[321]

d) Judicial review in EIO procedures

The judicial review procedure initiated by the person concerned is not changed by the law implementing the Directive EIO. This means that not only the judicial review by the individual is not regulated, but also the problems described under c) remain, e.g., the question on how the right to judicial review can be effectively protected (e.g., by the ban to use the intercepted material as evidence).[322] Furthermore, the individual has also in EIO procedures only indirect access to the court regarding the issue *whether* assistance could have been rendered.

The particularity in EIO procedures is, however, that the possibilities of the Higher Regional Court to carry out a review on the discretionary decisions (see Section 91i in connection with Sections 91e and 91f AICCM and supra b.) must also be recognised within the *Integrationslösung*. The legislator left to practice how the individual can influence the procedure before the court if he/she proceeds (subsequently) against the enforcement of the measure and which (legal) position the individual hass in the potential proceedings before the Higher Regional Court. In this context, the particular question arises, for instance, whether the individual has a right for own motions before the Higher Regional Court to request examinations

---

319 *Fabri/Fugger*, ZStR 2010, 394 (406).

320 *Ibid*.

321 See details in the German version of this project report.

322 Section 91i Subsection 2 AICCM stipulates that the transfer of evidence can be suspended until a decision is made on the legal remedy. This could be a legal remedy in the issuing Member State against the issuance of the EIO or a legal remedy filed under German law. However, this provision is not applicable for covert investigations (*Böse*, ZIS 2014, 52, 61).

of the discretionary decisions as stipulated in Section 91i Subsection 1 AICCM. Furthermore, it is debatable whether he/she is precluded from judicial review if the investigative judge at the local court had already initiated an MLA review before ordering the interception.

2. Outgoing requests

a) Regular procedure

In case of outgoing requests, two stages of the procedure must also principally be distinguished: In the first stage, it is the question of whether a MLA request for the interception of telecommunications should be issued to the foreign authorities. In the second stage, it is the question of whether the MLA request can be approved (procedure of approval – *Bewilligungsverfahren*).

In the first stage, the competent public prosecution service that investigates a criminal case decides whether an interception of telecommunications abroad is necessary in order to gather sufficient evidence.[323] The police or other law enforcement authorities may encourage the public prosecution service to file a MLA request, but cannot issue it themselves.

The competent public prosecutor can only issue a MLA request if the requirement(s) of the respective measure are fulfilled if it were to be enforced on German territory. Therefore, the competent public prosecutor must examine whether the lawfulness and appropriateness of the interception of telecommunications comply with the rules of the GCPC. In terms of substance, it is particularly necessary that (1) certain facts give rise to the suspicion that a person has committed a serious criminal offence referred to in Subsection 2 of Section 100a GCPC; and (2) the offence is one of particular gravity in the individual case as well; and (3) other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success. In formal terms, the public prosecution service must apply for an order to intercept telecommunications at the competent court.[324] The order of the court has no enforcement effects for the foreign authority, but corresponds to the relevant formal requirements in the interna-

---

[323] It is commonly the public prosecution service at the Regional Courts. Within its competence, the general prosecutor (public prosecutor at the Higher Regional Court) or the Federal Prosecutor General may also be the responsible prosecution service (cf. fn. 295).

[324] Section 100e Subsection 1 GCPC. In a conventional case, it is the investigative judge at the local court. In cases involving the competence of the Federal Prosecutor General, the investigative judge at the Federal Court of Justice is responsible; in cases involving the competence of the general prosecutor at the Higher Regional Court, it is the investigative judge at the Higher Regional Court. In exigent circumstances, the public prosecution office may also issue an order. However, such an order must be confirmed by the court within three working days (Section 100e Subsection 1 Sentences 2 and 3 GCPC).

tional MLA treaties, such as Article 18 Subsection 3 lit. b) MLA Convention EU (cf. supra).

The public prosecution service also prepares the MLA request. In particular, it must take into account all the formal requirements as stipulated in the applicable international agreement (e.g., Article 18 paras. 2 and 4 MLA Convention EU). The RiVASt contains general guidelines for the issuance of MLA requests to foreign countries (Nos. 25 et seq.).

At the beginning of the second stage of the procedure, the public prosecution service submits the drafted MLA request to the competent authority for approval. The authority responsible for approving the MLA request results from Section 74 AICCM in connection with the various decrees of the federal states (cf. supra). As a rule, the federal states delegated the competence for approving MLA requests addressed to EU Member States to the heads of the respective public prosecution service (commonly the chief public prosecutors).[325] Within the framework of the approval procedure, the competent authority (head of the public prosecution service) examines anew the lawfulness of the measure in accordance with the national law (code of criminal procedure) as well as the fulfillment of the requirements of the international MLA agreement that exists with the requested state at issue.

The approved/granted MLA request is transmitted to the competent foreign authorities via the foreseen channels (as stipulated in the international agreements, such as Article 6 MLA Convention EU).

The person concerned may proceed against the decision of the competent investigating public prosecution service to issue a MLA request after notification of the interception measure (Section 101 Subsection 7 Sentence 2 GCPC). It has not yet been clarified whether the person concerned may also contest the decision of approval and claim that the admissibility of the outgoing MLA request was not given. The majority of legal scholars negate that the decision of approval is subject to judicial review.[326] However, this question is rather theoretical. In legal practice, the question instead is whether the information collected by means of an interception of telecommunications abroad can be used as evidence in criminal proceedings against the defendant in Germany. This question is further explored in the following section 3.

---

[325] In case of the competence of the Federal Prosecutor General to investigate a criminal case, the authority responsible for approving the request is the Federal Office of Justice *(Bundesamt für Justiz)* according to Section 74 Subsection 1 AICCM in connection with No. 1 of the decree of the Federal Ministry of Justice of 2 January 2007 – II B 6 – BfJ –.

[326] *Schomburg/Hackner*, in: Schomburg/Lagodny/Gleß/Hackner, Internationale Rechtshilfe in Strafsachen, 5th ed. 2012, vor § 68 IRG, mn. 97.

b) Particularities in EIO procedures

As with incoming requests, the implementation of the Directive EIO does not change the principal structures and competences for outgoing EIOs. In particular, the two-step procedure as described under a) applies also in EIO procedures. As in conventional MLA cases, also the issuing of the EIO is linked to the general rules of the GCPC. Therefore, the German implementation law only includes brief provisions for outgoing requests in Section 91j AICCM.[327]

Section 91j Subsection 1 AICCM highlights that German authorities are obliged to use the forms in annexes A and C of the Directive EIO. In practice, German authorities must especially examine in which languages the request must be translated, in particular whether the executing state also accepts English beside its official language.[328]

Although not specifically regulated, Germany takes into account Article 6 Subsection 1 lit. b) Directive EIO which stipulates that the issuing authority may only issue an EIO where the condition is met that the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case. For EIOs applying for the interception of telecommunications this means in particular that the substantive and formal requirements as stipulated in Sections 100a and 100e GCPC must be met as in conventional MLA procedures. By contrast, it is not necessary in EIO cases to include the (national) judicial order into the request.[329] It is, however, recommended that German authorities attach the judicial order to the EIO because it can be helpful for the executing state to assess proportionality. Furthermore, it prevents subsequent requests for clarifications, thus avoiding delays in the execution of the request.

Section 91j Subsections 2–4 AICCM implement the validation requirements as set out in Article 2 lit. c) ii) Directive EIO if the EIO is issued by a German administrative authority. According to the German notification,[330] no validation procedure is requested if German fiscal authorities are independently conducting a criminal investigation pursuant to Section 386(2) Tax Code.

The judicial review of issued EIOs follows the same rules as in conventional MLA procedures. The general problem persists whether the decision of approval can be "attacked." Section 91i AICCM does not come into play here since it is exclusively designed for incoming requests only. The structure of the Germany sys-

---

[327] This is supplemented by Sections 213–215 RiVASt.

[328] See the practical information by the EJN (last updated 7 August 2019), available at https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties/EN/2120

[329] Cf. Article 30 para. 3 and Section H7 of form A Directive EIO.

[330] Cf. A.1.c.

tem to seek judicial review has neither been influenced by the Directive EIO nor the implementation law.[331]

3. Technical regulations of "customary" interception of telecommunications

German criminal procedure law contains several restrictions and prohibitions when it comes to the taking of evidence in the form of an interception of telecommunications. These restrictions and prohibitions serve to safeguard the civil liberties of suspects and/or uninvolved persons. The question arises as to whether these restrictions/prohibitions must also be observed in transnational cases. The following part deals with the "customary" interception of telecommunications by which German authorities wiretap someone and transmit the records to a foreign country afterwards. In these cases, the German authorities may examine the records before transmission to the foreign authority. Part 4 examines possible specifics in cases of real-time transmission of intercepted data to a foreign country. In each case, a distinction is first made between incoming and outgoing MLA requests for the surveillance of telecommunications. Second, in a first step, the problems in conventional MLA procedures are examined, whereas particularities that may be deducted from the Directive EIO are discussed subsequently.

a) Incoming requests

aa) Conventional MLA

The German law does not contain an explicit rule that regulates the observance of the restrictions and prohibitions of the taking of evidence within the framework of MLA. Specific, settled case law does not exist either. Therefore, one must resort to the general rules. In this context, one should take note of Section 59 Subsection 3 AICCM:

> Legal assistance may be provided only in those cases in which German courts and executive authorities could render mutual legal assistance to each other.

This provision formulates a general rule that the requested MLA measure can only be implemented if it complies with German national law. It means that rendering mutual legal assistance in criminal matters cannot be further than is lawfully possible in purely national cases. In other words: the national rules that apply to the enforcement of the MLA measure also set the legal boundaries for MLA to foreign countries.

The Federal Constitutional Court *(Bundesverfassungsgericht)* has established case law regarding the legal requirements for carrying out covert surveillance measures for purely national cases only. In a decision of 20 April 2016, which con-

---

331 *Brahms/Gut*, NStZ 2017, 388 (394).

solidated the established case law so far, the Federal Constitutional Court emphasised again that investigative powers, which lead to interference with the strictly protected core area of private life (including the interception of telecommunications), must be accompanied by particular protective rules.[332] These protective rules must be considered on two levels. First, at the level of data collection, precautionary measures must be established in order to exclude, as far as possible, the unintended acquisition of information on the core area of private life.[333] Second, at the level of the use of the data, it must be ensured that any unavoidably collected information relating to the core area of private life must be filtered out before use of the data.[334] This seems to back the viewpoint of legal scholars who deduce from Section 59 Subsection 3 that German rules restricting or prohibiting the taking of evidence *(Beweisverbote)* also block the transmission of the evidentiary result to a foreign state, at any rate if these rules implement constitutional safeguards of fundamental rights and civil liberties.[335] If a German authority is not entitled to use certain items of information for its own purposes, it is not even entitled to forward this information to other third parties in Germany, as a result of which it is not even possible to transfer information to foreign authorities.

Based on these statements, Germany would have filtering obligations if it comes to the transmission of "privileged information." In detail, this would mean:

i) The interception of telecommunications as a MLA measure for the foreign country must be denied, if there are factual indications for assuming that solely *(sic)* information concerning the core area of the private conduct of life would be acquired (Section 100d Subsection 1 GCPC).

ii) The records of the interception cannot be handed over if information concerning the core area of the private conduct of life is acquired during an interception of telecommunications (Section 100d Subsection 2 GCPC).

iii) The interception of telecommunications cannot be carried out if the interception is directed at a clergyman; defense counsel of the accused; members of the Federal Parliament, of the Federal Convention, of the European Parliament from the Federal Republic of Germany or of a *Land* parliament; an attorney; a person who has been admitted to a Bar Association pursuant to section 206 of the Federal Regulations for Practising Lawyers or a non-attorney provider of legal services who has been admitted to a Bar Association if it is expected to produce

---

[332] BVerfG, judgment of 20 April 2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781, mn. 119. An English summary of the decision is available at http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2016/bvg16-019.html

[333] BVerfG, *op. cit.* (fn. 332), mn. 126.

[334] BVerfG, *op. cit.* (fn. 332), mn. 129.

[335] *Oehmichen*, StV 2017, 257 (260); *Güntge*, in: Ambos/König/Rackow (eds.), Rechtshilferecht in Strafsachen, HT 4, mn. 2; *Trautmann/Zimmermann*, in: Schomburg/Lagodny, Internationale Rechtshilfe in Strafsachen, 6th ed., § 59 IRG, mn. 36

information in respect of which such person would have the right to refuse to testify (Section 160a Subsection 1 Sentence 1 GCPC).

iv) Records could not be handed over, if any information in the aforementioned cases iii) is obtained during the interception of telecommunications (Section 160a Subsection 1 Sentence 2 GCPC) or if information about a person referred to in Section 160a Subsection 1 Sentence 1 GCPC is obtained through an investigation measure that is not aimed at such person and in respect of which such person may refuse to testify (Section 160a Subsection 1 Sentence 5 GCPC).

v) The interception of telecommunications cannot be carried out if a person named in Section 53 Subsection (1) Sentence 1, numbers 3 to 3b or number 5 GCPC[336] might be affected by the investigation measure and it is to be expected that information would thereby be obtained in respect of which the person would have the right to refuse to testify, and an examination of the circumstances concludes that an interception is disproportionate (Section 160a Subsection 2 Sentence 1 GCPC).

vi) The records cannot be handed over if one of the aforementioned constellations v ccurs during the interception of telecommunications or the factual basis for the examination of proportionality has changed (Section 160a Subsection 2 Sentence 3 GCPC).[337]

As a consequence of these findings, the obligation to delete the obtained information as set by the law (Section 100a Subsection 4 Sentence 3; Section 160a Subsection 1 Sentence 2 GCPC) would also apply.

However, the strict application of the German rules on evidence gathering, even in MLA cases, leads to two inconsistencies. First, the Federal Constitutional Court regularly stresses that the Basic Law's alignment towards international cooperation

---

336 Section 53a (1) 1 No.
3: attorneys, patent attorneys, notaries, certified public accountants, sworn auditors, tax consultants and tax representatives, doctors, dentists, psychological psychotherapists, psychotherapists specializing in the treatment of children and juveniles, pharmacists, and midwives;
3a: members or representatives of a recognized counselling agency pursuant to Sections 3 and 8 of the Act on Pregnancies in Conflict Situations;
3b: drugs dependency counsellors in a counselling agency recognized or set up by an authority, a body, an institution or a foundation under public law, concerning the information that was entrusted to them or became known to them in this capacity;
5: individuals who are or have been professionally involved in the preparation, production or dissemination of periodically printed matter, radio broadcasts, film documentaries or in the information and communication services involved in instruction or in the formation of opinion.

337 Note: Section 160a GCPC does not apply where certain facts substantiate the suspicion that the person who is entitled to refuse to testify participated in the offence or in accessoryship after the fact, obstruction of justice or handling stolen goods (Section 160a Subsection 4 GCPC).

encompasses the respect for foreign legal orders and conceptions.[338] This is also why own constitutional requirements become valid in the event of international cooperation. As a result, German fundamental rights standards prevailing the national legal order cannot be fully upheld if Germany enters into international cooperation in criminal matters, and they do not fundamentally prevent the transfer of evidence to third countries, although German state authorities remain bound to respect the Basic Law's fundamental rights.[339] Second, in the reverse case, i.e., if Germany receives evidence obtained abroad on the basis of a German MLA request (see b. below), German courts principally ignore the rules on the gathering and use of evidence in the foreign country and apply the rule that the evidentiary law of the *forum* reigns if it comes to the use of evidence in Germany. An exception is made, however, if the gathering of evidence abroad contradicts the German public policy order *(ordre public)*, i.e., basic principles of the German legal order. Therefore, it may be questioned why Germany does not accept the *forum regit actum* principle, also in cases when it comes to the transfer of evidence collected in Germany.

Against this background, it remains open whether the above-mentioned obligations and guidelines can be maintained and whether other more flexible solutions could even be found.[340] Comprehensive obligations on the part of German authorities to examine the records of the interception and to filter out unlawful content are one of the disadvantages of the above-mentioned guidelines. This could render MLA for the interception of telecommunications more or less impracticable. Furthermore, it could be doubted whether a stringent applicability of the German restrictions and prohibitions on the taking of evidence strike the right balance between the obligations from international agreements (e.g., Article 18 Subsection 5 MLA Convention EU), the protection of civil liberties, and the interests of the participating states.

It could be deliberated whether the public policy exception *(ordre public)* could not serve as a limit for rendering MLA for the interception of telecommunications. The *ordre public* limit means that legal assistance cannot be granted if it would conflict with basic principles of German law.[341] Whether a rule of German criminal procedure is a "basic principle of German law" is subject to determination by case law. If this approach is followed, the German authorities would still have certain obligations to examine the information obtained and not to transmit information that contradicts the basic principles of German law. This would include information that affects the core area of the private conduct of life and information obtained from "privileged persons" (cf. supra). In contrast to the more stringent ap-

---

338 BVerfGE 63, 343 (370).

339 BVerfG, NJW 2016, 1781, mn. 325 et seq.

340 *Gleß*, in: Samson (ed.), Festschrift Grünwald, p. 197 (199), remarks that international cooperation in criminal matters often requires pragmatic solutions.

341 Cf. Article 2 lit. b) 1959 MLA Convention; Section 73 AICCM.

proach, the German authorities, however, may secure observance of the basic principles (in particular) by setting conditions (as foreseen in Article 18 Subsection 5 lit. b) MLA Convention EU and No. 77a RiVASt). These conditions would restrict the use of the privileged information in foreign criminal proceedings by the international rule of speciality. The setting of conditions would above all be necessary if the person concerned seeks subsequent judicial review by which a court could deem the transferred information not to be in line with the basic principles of German law.

In sum, the question of whether and to what extent there are obligations to filter out or delete "privileged information" is not easy to answer, since there is a lack of settled case law and clear statements in the literature for specific MLA cases of covert investigations by means of wiretapping. General statements so far seem to require a strict observance of the German criminal procedural rules that restrict or prohibit the taking of evidence by means of the interception of telecommunications. As a result, the German authorities would have comprehensive obligations to filter out and delete "privileged information," in particular information that concerns the "core area of the private conduct of life" or information that affects certain persons with the right to refuse testimony. Another approach, which is favored here, could be to assess first whether the German rule affects the German *ordre public*, i.e., the basic principles of German law. In the affirmative and as a second step, German authorities could make the use of privileged information dependent on conditions vis-à-vis the requesting state.

bb) Particularities due to the Directive EIO

The fundamental problems as discussed under aa) are equally posed when the Directive EIO is applied. As a rule, the new EU framework based on the principle of mutual recognition of judicial decision does not include a solution on the intricate legal problems that have been posed in the conventional MLA situations. The reason is that Article 30 Directive EIO is largely aligned to its predecessor in Article 18 MLA Convention EU. Article 30 does not change the system that in cases of interception of telecommunications reference is made "back" to the national legal systems. Hence, Section 91c AICCM explicitly clarifies that the conditions set out in Section 59 Subsection 3 AICCM also apply for the interception of telecommunications based on an EIO request. In other words, Section 59 Subsection AICCM remains the starting point for any solutions to be found.

However, the plea for a more flexible approach not restricting the transfer of potentially spoiled evidence from the outset is reinforced by the underlying principle of mutual recognition. This principle implies, as a rule, that the question on the legality or illegality of the requested investigative measure (here: interception of

telecommunications) under a purely domestic situation is irrelevant at the outset.[342] Article 9 Directive EIO expresses this idea:

> The executing authority shall recognise an EIO, transmitted in accordance with this Directive, without any further formality being required, and ensure its execution in the same way and under the same modalities as if the investigative measure concerned had been ordered by an authority of the executing state, unless that authority decides to invoke one of the grounds for non-recognition or non-execution or one of the grounds for postponement provided for in this Directive.

A non-transmittance of intercepted telecommunications data to the issuing EU Member State because of German exclusionary evidence rules is not a ground for refusal or postponement.

It was submitted above that German concerns on the encroachment on the fundamental rights can be mitigated by setting corresponding conditions to the issuing authority/EU Member State. The question arose in Germany whether setting conditions is admissible in the EIO context because the provision of the Directive EIO explicitly authorizing this possibility of making conditions "which would have to be observed in a similar domestic case" (Article 30 Subsection 5 sentence 2 Directive EIO) was not taken up in the implementing law. However, the explanatory report of the bill clarifies that the making of conditions should be considered included as *maiore ad minus* in the implementing norm.[343] Thus, there will be no change to the current possibilities for the German authorities to make the consent of an interception of telecommunications subject to conditions, as already foreseen in Article 18 Subsection 5 MLA Convention EU and No. 77a Subsection 1 RiVASt (cf. supra).

b) Outgoing requests

aa) Conventional MLA

There are no specific legal rules on whether German authorities have a duty to filter out or to delete information that could not be intercepted according to German laws (or even acc. to the law of the sending state) due to a legal privilege accorded to Germany if it is the requesting state and later receives the results of the requested interception measure. However, the problem in Germany is considered less a question of duties to filter out or to delete information but rather an issue of whether the received information can be used as evidence in the trial before the German criminal court. In this context, the Federal Court of Justice *(Bundesgerichtshof)* – Germany's highest court of civil and criminal jurisdiction – dealt with the use of evi-

---

342 See, e.g., *Zimmermann/Glaser/Motz*, EuCLR 2011, 56 (60).

343 See also RegE EEA, *op. cit.* (fn. 268), p. 47.

dence of intercepted telecommunication information in a decision of 2012.[344] Although the underlying facts of the decision did not concern the interception of telecommunications of a person abroad on the basis of a targeted German MLA request, but instead the handing over of records by Czech authorities of intercepted data that had initially been obtained for the purpose of criminal proceedings in the Czech Republic (preserved data already in the possession of the Czech authorities), the Federal Court of Justice set important guidelines that also apply to other constellations. The Federal Court of Justice reiterated its standpoint that the question of the use of evidence obtained abroad must follow the rules of the requesting state, i.e., German law in the case at issue. In other words: the Federal Court of Justice applies the *forum regit actum* principle when it comes to the use of evidence instead of the *locus regit actum* principle, which applies to the enforcement of a requested MLA measure in Germany (cf. B.1.a.).

The Federal Court of Justice further emphasised that – as far as judicial cooperation within the EU is concerned (and there are no indications of abusive actions of the public authorities) – the use of the evidence obtained abroad is independent of the lawfulness of the measure in the requested EU state (here: the law of the Czech Republic). The Federal Court of Justice mainly argues that, in an area like the EU, which is footed on the principle of mutual recognition of judicial decisions, Germany is not entitled to examine the compliance of the measure at issue with the law of the enforcing state. As a consequence, it is not relevant if the requested state does not comply with the protection of privileged information in accordance with its law or other substantive or formal requirements of its law. In contrast, the received information cannot be used as evidence in German criminal procedure if the content of the information is affected by an exclusionary rule of German (criminal procedural) law. This would be the case if, e.g., the received information involves the core area of the private conduct of life or conversation with privileged persons pursuant to Section 160a GCPC.

In general, one must conclude, however, that many questions on an exclusion of collected evidence in the specific constellations of covert trans-border investigative measures – e.g., the interception of telecommunications – have not been decided by German supreme courts yet.[345] The approach is very casuistic, strict rules when evidence collected abroad can be used in the trial do not exist. In recent years, there is the general tendency of the courts that German authorities should request compliance with the formalities and procedures if this is legally possible.[346] Pursuant to Article 4 Subsection 1 MLA Convention EU and Article 8 Second Protocol of the

---

344 BGH 1 StR 310/12 – decision of 21 November 2012 (LG Hamburg) = BGHSt 58, 32 = HRRS 2013, Nr. 314.

345 See details at the German version of this report. For the various constellations instructive *Gless*, JR 2008, 317 (319).

346 BGHSt 42, 86 (91).

CoE MLA Convention this legal possibility is frequently the case in conventional MLA with European states. According to legal literature, formalities and procedures encompass German rules on the use of evidence if they can be deducted from fundamental rights, e.g., privileged information by professionals that is based on particular relationship of trust or the "core area privilege."[347] Older case law let also conclude that gained evidence may turn inadmissible if the German authorities "instigated" the foreign authorities to circumvent formalities and procedures under German law or omitted the request for compliance.[348]

bb) Particularities due to the EIO

In principle, the Directive EIO has not brought any change of the legal issues discussed under a). The main argument is that the Directive EIO does not include any provisions on the use of evidence in the various legal orders of the EU Member States. The obligation to comply with formalities and procedures is stipulated in Article 9 Subsection 2 Directive EIO. Legal literature discusses, however,[349] whether the Federal Court of Justice's approach in its 2012 landmark judgment that the lawfulness of the measures under the law of the requested/executing state is irrelevant is (still) in line with the provision in Article 14 Subsection 7 Directive EIO.[350]

4. Real-time transfer of communication data

a) Incoming requests

Real-time transfer of telecommunication data is possible in Germany. It is possible both on the basis of Union law (Article 30 Subsection 6 Directive EIO), an international agreement, such as Article 18 MLA Convention EU[351] and – upon individual agreement on details with the requesting state – on the basis of Article 59 AICCM. This is confirmed by No. 77a Subsection 1 and (implicitly) No. 2 RiVASt.

---

[347] *Oehmichen/Weißenberger*, StraFo 2017, 316 (323); *Böse,* ZIS 2014, 152 (154); *Schuster*, ZIS 2016, 564 (567).

[348] BGH NStZ 1988, 563; *Gleß*, FS Grünwald, p. 204.

[349] Instructive: *Böse*, ZIS 2014, 152 (162 et seq.).

[350] "The issuing State shall take into account a successful challenge against the recognition or execution of an EIO in accordance with its own national law. Without prejudice to national procedural rules Member States shall ensure that in criminal proceedings in the issuing State the rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the EIO."

[351] By consenting to the MLA Convention EU in the form of federal law, Germany entered into an obligation to render MLA in the form of the real-time transfer of communication data with the other EU Member State to which the Convention is applicable.

Also in this case, however, the German authorities are obliged to observe the restrictions and prohibitions stipulated by German criminal procedure law and to secure their observance vis-à-vis the requesting state as is the case for the "customary" method of interception of telecommunications. The particularity with regard to the real-time transfer of communication data is that German authorities are only able to fulfill their duties by establishing conditions pursuant to Article 30 Subsection 5 Directive EIO or Article 18 Subsection 5 MLA Convention EU, unless – at the moment of the enforcement of the MLA request – it is already clear that "privileged information" would be collected. An intervention before the transmission begins is hardly possible.

In purely national cases, the Federal Constitutional Court *(Bundesverfassungsgericht)* established various requirements that compensate interference into the civil liberties of the person concerned (in particular, Article 10 GG [Privacy of correspondence, posts and telecommunications]), e.g., labelling requirements for intercepted data, notification, deletion of no longer needed data, exclusionary rules for "privileged information," etc. It is still open whether the establishment of conditions in transnational cases (MLA cases) can be regarded as a sufficient compensation measure for interference into the civil liberties of the person concerned.[352] In the personal view of the author, conditions as foreseen in Article 30 Subsection 5 Directive EIO or Article 18 Subsection 5 MLA Convention EU are possible in order to safeguard German fundamental rights standards, also vis-à-vis foreign EU states (cf. B.3.a. above). The EIO scheme is actually an additional argument in favour of this view because constitutional yardsticks that fully apply in purely domestic cases cannot be upheld in a system of reinforced cooperation based on the principle of mutual recognition.[353] At the moment, however, this approach is not explicitly backed by German law or case law.

b) Outgoing requests

As mentioned above (B.3.b.), the concrete question is whether received information can be used as evidence in the criminal proceedings. This question is mainly addressed to the public prosecutor who prepares the indictment and to the criminal court that sits in trial. Insofar, there are no peculiarities between the real-time transfer of intercepted communications data and the "customary" surveillance of telecommunication by which records are transmitted and analysed. The principles as established by the Federal Court of Justice apply. The Directive EIO did not entail any change with regard to this legal issue (cf. B.3.b.).

---

352 See also B.3.a. above.

353 See in particular the CJEU's *Melloni* judgment of 26 February 2013, Case C-399/11.

C. Statistics

There are no official statistics available from the German executive authorities as far as "other" mutual legal assistance in criminal matters is concerned.

Appendix

Legislation

Serious criminal offences for the purpose of Section 100a subsection 1 number 1 StPO[354] shall be:

1. Pursuant to the German Criminal Code:

a) crimes against peace, high treason, endangering the democratic state based on the rule of law, treason and endangering external security pursuant to sections 80 to 82, 84 to 86, 87 to 89a and 94 to 100a:
   - Section 80 Preparation of a war of aggression, Section 80a Incitement to a war of aggression, Section 81 High treason against the Federation, Section 82 High treason against a member state,
   - Section 84 Continuation of a political party declared unconstitutional, Section 85 Violation of a ban on forming an association, Section 86 Distribution of propaganda material of unconstitutional organisations,
   - Section 87 Acting as a secret agent with the aim of sabotage, Section 88 Sabotage against the constitution, Section 89 Exerting anti-constitutional influence on the Armed Forces and public security forces, Section 89a Preparation of a serious violent offence endangering the state,
   - Section 94 Treason, Section 95 Disclosure of state secrets with intent to cause damage, Section 96 Treasonous espionage, spying on state secrets, Section 97 Disclosure of state secrets and negligently causing danger, Section 97a Disclosure of illegal secrets, Section 97b Disclosure based on mistaken assumption that secret is illegal, Section 98 Treasonous activity as an agent, Section 99 Working as an agent for an intelligence service, Section 100 Engaging in relations that endanger peace, Section 100a Treasonous forgery;

b) taking of bribes by, and offering of bribes to, mandate holders pursuant to section 108e,

c) crimes against the national defence pursuant to sections 109d to 109h:
   - Section 109d Disruptive propaganda against the Armed Forces, Section 109e Sabotage against means of defence, Section 109f Intelligence activity endangering national security, Section 109g Taking or drawing pictures etc. endangering national security, Section 109h Recruiting for foreign armed forces;

d) crimes against public order pursuant to sections 129 to 130:

---

[354] Based on the translation of the Federal Ministry of Justice and Consumer Protection by Brian Duffett, Monika Ebinger, Kathleen Müller-Rostin and Iyamide Mahdi, translation includes amendments to the Act by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I p. 410).

- Section 129 Forming criminal organisations, Section 129a Forming terrorist organisations, Section 129b Criminal and terrorist organisations abroad; extended confiscation and deprivation, Section 130 Incitement to hatred;

e) counterfeiting money and official stamps pursuant to sections 146 and 151, in each case also in conjunction with section 152, as well as section 152a subsection (3) and section 152b subsections (1) to (4):
   - Section 146 Counterfeiting money, Section 151 Securities, Section 152 Foreign money, stamps and securities, Section 152a subsection (3) Commercial or gang counterfeiting of debit cards, etc., cheques, and promissory notes, Section 152b subsections (1) to (4) Counterfeiting of credit cards with guaranteed payment, etc., and blank eurocheque forms;

f) crimes against sexual self-determination in the cases referred to in sections 176a, 176b, 177 subsection (2), number 2, and section 179 subsection (5), number 2:
   - Section 176a Aggravated child abuse, Section 176b Child abuse resulting in death, Section 177 subsection (2), number 2 Sexual assault committed jointly, Section 179 subsection (5), number 2 Abuse of persons incapable of resistance committed jointly.

g) distribution, acquisition and possession of pornographic writings involving children and involving juveniles, pursuant to section 184b subsections (1) to (3), section 184c subsection (3):
   - Section 184b subsections (1) to (3) Distribution, acquisition and possession of pornographic writings involving children, Section 184c subsection (3) Distribution, acquisition and possession of pornographic writings involving juveniles reproducing an actual or realistic activity on a commercial basis or as a member of a gang;

h) murder and manslaughter pursuant to sections 211 and 212,

i) crimes against personal liberty pursuant to sections 232 to 233a, 234, 234a, 239a and 239b:
   - Section 232 Trafficking in human beings for the purpose of sexual exploitation, Section 233 Trafficking in human beings for the purpose of exploitation of labour, Section 233a Assisting in trafficking in human beings, Section 234 Abduction, Section 234a Causing a danger of political persecution through use of force, threats or deception, Section 239a Abduction for the purpose of extortion, Section 239b Taking of hostages;

j) gang theft pursuant to section 244 subsection (1), number 2, and aggravated gang theft pursuant to section 244a,

k) crimes of robbery or extortion pursuant to sections 249 to 255:
   - Section 249 Robbery, Section 250 Aggravated robbery, Section 251 Robbery resulting in death, Section 252 Theft and use of force to retain stolen goods, Section 253 Extortion, Section 255Extortion resembling robbery;

l) commercial handling of stolen goods, gang handling of stolen goods and commercial gang handling of stolen goods pursuant to sections 260 and 260a,

m) money laundering or concealment of unlawfully acquired assets pursuant to section 261 subsections (1), (2) and (4), under exclusion of the attempt and less serious cases.

n) fraud and computer fraud subject to the conditions set out in section 263 subsection (3), sentence 2, and in the case of section 263 subsection (5), each also in conjunction with section 263a subsection (2):
   - Section 263 subsection (3), sentence 2 Particularly serious case of fraud resulting in major financial loss, Section 263 subsection (5) Commercial and gang fraud, also in conjunction with Section 263a Computer fraud;

o) subsidy fraud subject to the conditions set out in section 264 subsection (2), sentence 2, and in the case of section 264 subsection (3), in conjunction with section 263 subsection (5):

– Particularly serious cases of subsidy fraud/ Commercial and gang subsidy fraud;

p) criminal offences involving falsification of documents under the conditions set out in section 267 subsection (3), sentence 2, and in the case of section 267 subsection (4), in each case also in conjunction with section 268 subsection (5) or section 269 subsection (3), as well as pursuant to sections 275 subsection (2) and section 276 subsection (2):

– Section 267 subsection (3), sentence 2 Particularly serious case of falsification of documents, Section 267 subsection (4) Commercial and gang falsification of documents, Section 268 Falsification of technical records, Section 269 Falsification of data intended to provide proof, Section 275 Preparatory acts to tampering with official identity documents, Section 276 Acquisition of false official identity documents.

q) bankruptcy subject to the conditions set out in section 283a, sentence 2:

– Particularly serious cases of bankruptcy.

r) crimes against competition pursuant to section 298 and, subject to the conditions set out in section 300, sentence 2, pursuant to section 299:

– Section 298 Restricting competition through agreements in the context of public bids,

– Sections 299, 300 sentence 2 Particularly serious cases of taking and offering bribes in commercial practice, i.e., if the offence relates to a major benefit or the offender acts on a commercial basis or as a member of a gang;

s) crimes endangering public safety in the cases referred to in sections 306 to 306c, section 307 subsections (1) to (3), section 308 subsections (1) to (3), section 309 subsections (1) to (4), section 310 subsection (1), sections 313, 314, 315 subsection (3), section 315b subsection (3), as well as sections 316a and 316c:

– Section 306 Arson, Section 306a Aggravated arson, Section 306b Particularly aggravated arson, Section 306c Arson resulting in death,

– Section 307 Inducing a nuclear explosion,

– Section 308 Inducing an explosion, Section 309 Misuse of ionising radiation,

– Section 310 subsection (1) Acts preparatory to inducing an explosion or radiation offence,

– Section 313 Inducing flooding, Section 314 Inducing a common danger by poisoning, Section 315 subsection (3) Dangerous disruption of rail, ship and air traffic,

– Section 315b subsection (3) Dangerous disruption of road traffic,

– Section 316a Attacking a driver for the purpose of committing a robbery; Section 316c Attacks on air and maritime traffic;

t) taking and offering a bribe pursuant to sections 332 and 334.

Other serious offences pursuant to supplementary criminal statutes:

2. Pursuant to the Fiscal Code:

a) tax evasion under the conditions set out in section 370 subsection (3), sentence 2, number 5:

– Particularly serious case of tax evasion where the perpetrator as a member of a gang formed for the purpose of repeatedly committing acts pursuant to section 370 subsection (1), understates value-added taxes or excise duties or derives unwarranted VAT or excise duty advantages.

b) commercial, violent and gang smuggling pursuant to section 373,

c) handling tax-evaded property as defined in section 374 subsection (2):
– Commercial or gang handling tax-evaded property.

3. Pursuant to the Pharmaceutical Products Act:

criminal offences pursuant to section 95 subsection (1), number 2a, subject to the conditions set out in section 95 subsection (3), sentence 2, number 2, letter b,

– Placing on the market or prescribing medicinal products for doping purposes in the field of sport or administering such medicinal products to others commercially or as a member of a gang.

4. Pursuant to the Asylum Procedure Act:

a) inducement of an abusive application for asylum pursuant to section 84 subsection (3)
– committed commercially or as a member of a gang;

b) commercial *and* gang inducement of an abusive application for asylum pursuant to section 84a.

5. Pursuant to the Residence Act:

a) smuggling of aliens pursuant to section 96 subsection (2):
– in particularly serious cases: committed commercially or as a member of a gang, subjection of the smuggled persons to potentially fatal, inhumane or humiliating treatment or a risk of sustaining severe damage to their health.

b) smuggling resulting in death and commercial and gang smuggling pursuant to section 97.

6. Pursuant to the Foreign Trade and Payments Act:

wilful criminal offences pursuant to sections 17 and 18 of the Foreign Trade and Payments Act:

– Section 17 subsection (1) Violation of an ordinance serving to implement an economic sanction adopted by the Security Council of the United Nations under Chapter VII of the Charter of the United Nations or by the Council of the European Union in the field of Common Foreign and Security Policy related to weapons, ammunition and equipment goods, to the extent the ordinance provides for criminal punishment; Note that Section 17 subsections (2) et seqq. include both less serious as well as particularly serious cases of Section 17 subsection (1),
– Section 18 subsection (1) Violation of a prohibition on or a licensing requirement for the export, import, transit, transfer, sale, acquisition, delivery, provision, passing on, service or investment or prohibition on the disposal of frozen money and economic assets of a directly applicable act of the European Communities or the European Union published in the Official Journal of the European Communities or the European Union which serves to implement an economic sanction adopted by the Council of the European Union in the field of Common Foreign and Security Policy,
– Section 18 subsection (2) Violation of the Foreign Trade and Payments Ordinance by (e.g.)

  (a) exporting goods cited in it without a license – mostly again weapons, ammunition and equipment goods,

  (b) undertaking a trafficking and brokering transaction without a license,

  (c) providing technical support without a license;

– Section 18 subsection (3) et seqq. Violation of Council Regulation (EC) No. 2368/2002 of 20 December 2002 implementing the Kimberley Process certification scheme for the international trade in rough diamonds (OJ L 358 of 31 December 2002, p. 28), most recently amended by Regulation (EC) No. 1268/2008 (OJ L 338 of 17 December 2008), by importing rough diamonds in violation of Article 3 or exporting rough diamonds in violation of Article 11.

7. Pursuant to the Narcotics Act:

a) criminal offences pursuant to one of the provisions referred to in section 29 subsection (3), sentence 2, number 1, subject to the conditions set out therein:
   – i.e., commercial commission of certain narcotics-related offences;

b) criminal offences pursuant to section 29a, section 30 subsection (1), numbers 1, 2 and 4, as well as sections 30a and 30b:
   – Section 29a Particularly serious cases: illicitly supplying narcotic drugs to a person under the age of 18 as a person over the age of 21 or, in contravention of section 13 subsection 1, administering them to such a person or putting them at their disposal for immediate use; illicitly trading, producing or supplying narcotic drugs in quantities which are not small,
   – Section 30 subsection (1) number 1 illicitly trading, producing or cultivating narcotic drugs as a member of a gang, number 2 supplying narcotic drugs to a person under the age of 18 as a person over the age of 21 on a commercial basis, number 4 importing of narcotic drugs in quantities which are not small,
   – Section 30a illicitly trading, producing, cultivating or importing/exporting narcotic drugs in quantities which are not small, acting as a member of a gang; as a person over the age of 21 causing a person under the age of 18 to illicitly trade in narcotic drugs; illicitly trading in narcotic drugs in quantities, which are not small and so doing, carrying a firearm,
   – Section 30b criminal association for the purpose of unauthorised international distribution of narcotic drugs.

8. Pursuant to the Precursors Control Act:

   criminal offences pursuant to section 19 subsection (1), subject to the conditions set out in section 19 subsection (3), sentence 2:
   – Violation of the Precursors Control Act or of EU-Regulation No. 273/2004 or EU Regulation No. 111/2005, i.e., commercial or gang illegal handling of basic materials used for the production of narcotic drugs.

9. Pursuant to the War Weapons Control Act:

a) criminal offences pursuant to section 19 subsections (1) to (3) and section 20 subsections (1) and (2), as well as section 20a subsections (1) to (3), each also in conjunction with section 21,
   – illegal handling of weapons of mass destruction, mines and cluster ammunition, including the facilitation or enticement of such handling; this is also punishable when committed abroad, provided the perpetrator is a German citizen; exclusion of criminal liability based on negligence.

b) criminal offences pursuant to section 22a subsections (1) to (3),
   – illegal handling of war weapons under exclusion of liability based on negligence.

10. Pursuant to the Code of Crimes against International Law:

a) genocide pursuant to section 6,

b) crimes against humanity pursuant to section 7,

c) war crimes pursuant to sections 8 to 12.

11. Pursuant to the Weapons Act:

a) criminal offences pursuant to section 51 subsections (1) to (3):
   – illegal handling of guns for shooting fixed ammunition, both in particularly serious (commercial or gang commission) as well as in less serious cases;

b) criminal offences pursuant to section 52 subsection (1), number 1 and number 2, letters c and d, as well as section 52 subsections (5) and (6).

Bibliography

Albrecht, Florian/Braun, Frank, Die strafprozessuale Überwachung des Surfverhaltens. HRRS 2013, 500 et seq.

Ahlbrecht, Heiko/Böhm, Klaus Michael/Esser, Robert/Hugger, Heiner/Rosenthal, Michael, Internationales Strafrecht in der Praxis. 2nd edition. Munich 2016.

Ambos, Kai/König, Stefan/Rackow, Peter (eds.), Rechtshilfe in Strafsachen. Baden-Baden 2015.

Arndt, Hans-Wolfgang, Telekommunikationsgesetz: Kommentar. 2nd edition. Berlin 2015.

Arndt, Hans-Wolfgang/Fademrecht, Thomas (eds.), Berliner Kommentar zum Telekommunikationsgesetz. 2nd edition. Berlin 2015 (cited as BerlKommTKG/*author*).

Bär, Wolfgang, Die Neuregelung des § 100j StPO zur Bestandsdatenauskunft – Auswirkungen auf die Praxis der Strafverfolgung. MMR 2013, 700 et seq.

Becker, Christian/Meinicke, Dirk, Die sog. Quellen-TKÜ und die StPO – von einer „herrschenden Meinung" und ihrer fragwürdigen Entstehung. StV 2011, 50 et seq.

Beck'scher Online-Kommentar zur Strafprozessordnung, see *Graf, Jürgen Peter.*

Beck'scher TKG-Kommentar zum Telekommunikationsgesetz, see *Geppert, Martin/ Schütz, Raimund* (eds.).

Berliner Kommentar zum Telekommunikationsgesetz, see *Arndt, Hans-Wolfgang/Fademrecht, Thomas* (eds.).

Böckenförde, Thomas, Auf dem Weg zur elektronischen Privatsphäre. JZ 2008, 925 et seq.

Boehm, Franziska/Andrees, Markus, Zur Vereinbarkeit der Vorratsdatenspeicherung. CR 2016, 146 et seq.

Böse, Martin, Die Europäische Ermittlungsanordnung – Beweistransfer nach neuen Regeln? ZIS 2014, 152 et seq.

Brahms, Katrin/Gut, Till, Zur Umsetzung der Richtlinie Europäische Ermittlungsanordnung in das deutsche Recht – Ermittlungsmaßnahmen auf Bestellschein? NStZ 2017, 388 et seq.

Braun, Frank, Überwachung des Surfverhaltens nach den §§ 100a, 100b StPO zulässig. jurisPR-ITR 18/2013.

Brodowski, Dominik, Strafprozessualer Zugriff auf E-Mail-Kommunikation. JR 2009, 402 et seq.

– Anmerkung zum Urteil des LG Landshut, Beschluss vom 20.1.2011 – 4 Qs 346/10. JR 2011, 533 et seq.

Brunst, Phillip, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen. Berlin 2009.

Buermeyer, Ulf/Bäcker, Matthias, Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO. HRRS 2009, 433 et seq.

Denninger, Erhard/Rachor, Frederik, Handbuch des Polizeirechts. 5th edition. Munich 2012.

Eisenberg, Ulrich/Singelnstein, Tobias, Zur Unzulässigkeit der heimlichen Ortung per „stiller SMS". NStZ 2005, 62 et seq.

Erbs, Georg/Kohlhaas, Max, Strafrechtliche Nebengesetze. 227th supplement. Munich 2019.

Geppert, Martin/Schütz, Raimund (eds.), Beck'scher TKG-Kommentar – Telekommunikationsgesetz. 4th edition. Munich 2013 (cited as BeckTKG-Komm/*author*).

Gleß, Sabine, Das Verhältnis von Beweiserhebungs- und Beweisverwertungsverboten und das Prinzip „locus regit actum". In: Erich Samson (ed.), Festschrift für Gerald Grünwald zum 70. Geburtstag. Baden-Baden 1999, pp. 197 et seq.

Gless, Sabine, Beweisverbote in Fällen mit Auslandsbezug. JR 2008, 317 et seq.

Graf, Jürgen Peter, Beck'scher Online-Kommentar Strafprozessordnung. 35th edition. Munich 2019 (cited as Beck-OK/*author*).

Hackner, Thomas/Schierholt, Christian, Internationale Rechtshilfe in Strafsachen. 3rd edition. Munich 2017.

Hannich, Rolf (ed.), Karlsruher Kommentar zur Strafprozessordnung. 7th edition. Munich 2013 (cited as KK/*author*).

Hiéramente, Mayeul, Legalität der strafprozessualen Überwachung des Surfverhaltens. StraFo 2013, 96 et seq.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (eds.), Handbuch Multimedia-Recht. 50th edition. Munich 2020. EL 46 January 2018, part 19.3 paras. 119–121.

Karlsruher Kommentar zur Strafprozessordnung, see *Hannich, Rolf* (ed.).

Kindhäuser, Urs/Neumann, Ulfried/Paeffgen, Hans-Ullrich (eds.), Strafgesetzbuch. 4th edition. Munich 2013 (cited as NK/*author*).

Klein, Oliver, Offen und (deshalb) einfach – Zur Sicherstellung und Beschlagnahme von E-Mails beim Provider. NJW 2009, 2996 et seqq.

Klesczewski, Diethelm, Straftataufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingriffen im Internet. ZStW 123 (2011), 737 et seqq.

Kudlich, Hans, Strafverfolgung im Internet – Bestandsaufnahme und aktuelle Probleme. GA 2011, 193 et seq.

Löwe, Ewald/Rosenberg, Werner, Die Strafprozessordnung und das Gerichtsverfassungsgesetz. 26th edition. Berlin/Boston 2014.

Maunz, Theodor/Dürig, Günther, Grundgesetz. 88. Ergänzungslieferung. Munich 2019.

Meinicke, Dirk, Anmerkung zum Urteil des AG Reutlingen, Beschluss vom 31.10.2011 – 5 Ds 43 JS 18155/10 jug. StV 2012, 463 et seq.

Meyer-Goßner, Lutz/Schmitt, Bertram, Strafprozessordnung. 62nd edition. Munich 2019.

Nomos Kommentar zur Strafprozessordnung, see *Kindhäuser, Urs/Neumann, Ulfried/Paeffgen, Hans-Ullrich* (eds.).

Oehmichen, Anna, Verfassungs- und europarechtliche Grenzen der Auslieferung. StV 2017, 257 et seq.

Oehmichen, Anna/Weißenberger, Björn, Die Europäische Ermittlungsanordnung – praxisrelevante Aspekte der deutschen Umsetzung im IRG. StraFo 2017, 316 et seq.

Park, Tido, Handbuch Durchsuchung und Beschlagnahme. 2nd edition. Munich 2009.

Pfeiffer, Gerd, Strafprozessordnung. 5th edition. Munich 2005

Roßnagel, Alexander, Die neue Vorratsdatenspeicherung. NJW 2016, 533 et seq.

Roxin, Claus/Schünemann, Bernd, Strafverfahrensrecht. 28th edition. Munich 2014.

Schenke, Wolf-Rüdiger, Polizei- und Ordnungsrecht. 8th edition. Heidelberg, Munich a.o. 2013.

Schomburg, Wolfgang/Lagodny, Otto, Internationale Rechtshilfe in Strafsachen. 6th edition. Munich 2020.

Schönke, Adolf/Schröder, Horst, Strafgesetzbuch. 29th edition. Munich 2014 (cited as Schönke/Schröder/*author*).

Schuster, Frank Peter, Verwertbarkeit von Beweismitteln bei grenzüberschreitender Strafverfolgung. ZIS 2016, 564 et seq.

Sieber, Ulrich, Straftaten und Strafverfolgung im Internet – Gutachten zum 69. Deutschen Juristentag. Munich 2012.

Singelnstein, Tobias, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co. NStZ 2012, 593 et seq.

Systematischer Kommentar zur Strafprozessordnung, see *Wolter, Jürgen* (ed.).

Wolter, Jürgen (ed.), Systematischer Kommentar zur Strafprozessordnung. 4th edition. Munich 2011 (cited as *author*, in: SK-StPO).

Zimmermann, Frank/Glaser, Sanja/Motz, Andreas, Mutual Recognition and its Implications for the Gathering of Evidence in Criminal Proceedings: a Critical Analysis of the Initiative for a European Investigation Order. EuCLR 2011, 56 et seq.

List of Abbreviations

AG	Amtsgericht
AICCM	Act on International Cooperation in Criminal Matters of 23 December 1982 (Gesetz über die internationale Rechtshilfe in Strafsachen)
BayLT	Bayrischer Landtag (Bavarian state parliament)
BayPAG	Bayrisches Polizeiaufgabengesetz (Bavarian police law)
BDSG	Bundesdatenschutzgesetz (Federal Data Protection Act)
Beck-OK StPO	Beck'scher Online-Kommentar zur Strafprozessordnung (legal commentary)
BeckTKG-Komm	Beck'scher Kommentar zum Telekommunikationsgesetz (legal commentary)
BerlKommTKG	Berliner Kommentar zum Telekommunikationsgesetz (legal commentary)
BfV	Bundesamt für Verfassungsschutz (German Domestic Intelligence Service)
BGH	Bundesgerichtshof (Federal Court of Justice)
BKAG	Bundeskriminalamtsgesetz (Federal Bureau of Investigation Act)
BND	Bundesnachrichtendienst (Federal Intelligence Agency)
BNDG	Bundesnachrichtendienstgesetz (Federal Intelligence Agency Act)
BMWi	Bundesministerium für Wirtschaft und Energie (Federal Ministry for Economic Affairs and Energy)
BT-Drs.	Bundestagsdrucksache (parliamentary document)
BVerfG	Bundesverfassungsgericht (Federal Constitutional Court)
BverfGE	Bundesverfassungsgerichtsentscheidung (Decision of the Federal Constitutional Court)
BVerfSchG	Bundesverfassungsschutzgesetz (domestic intelligence law)
BvR	Aktenzeichen einer Verfassungsbeschwerde zum Bundesverfassungsgericht (File number of the Constitutional Court)
BWPolG	Polizeigesetz Baden-Württemberg (Police law of Baden-Württemberg)
CR	Computer und Recht (law journal)
ECJ	European Court of Justice
EIO	European Investigation Order
ErmR	Ermittlungsrichter (investigating judge)

EuGH	Europäischer Gerichtshof (European Court of Justice)
G 10	Gesetz zur Beschränkung des Post-, Brief- und Fernmeldegeheimnisses (Act Restricting the Secrecy of the Post, of Letters, and of Telecommunication)
GA	Goltdammer's Archiv (law journal)
GCPC	German Criminal Procedure Code
GG	Grundgesetz (German Basic Law)
GVG	Gerichtsverfassungsgesetz (Courts Constitution Act)
HamPolG	Hamburger Polizeigesetz (Police law of Hamburg)
HessSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (Police law of Hessen)
HRRS	Online-Zeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht (law journal)
HSOG	Hessisches Sicherheits- und Ordnungsgesetz (Police law of Hesse)
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IRG	(see AICCM)
JR	Juristische Rundschau (law journal)
jurisPR-ITR	juris-Praxisreport IT-Recht (law journal)
JZ	Juristenzeitung (law journal)
KK	Karlsruher Kommentar zur Strafprozessordnung (legal commentary)
KG	Kammergericht
LG	Landgericht (District Court)
MLA	mutual legal assistance in criminal matters
MMR	Multimedia und Recht (law journal)
NdsSOG	Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (Police law of Lower Saxony)
NJOZ	Neue Juristische Online-Zeitschrift (law journal)
NJW	Neue Juristische Wochenschrift (law journal)
NK	Nomos Kommentar zur Strafprozessordnung (legal commentary)
NStZ	Neue Zeitschrift für Strafrecht (law journal)
OLG	Oberlandesgericht
POG RP	Polizeigesetz Rheinland-Pfalz (Police law of Rhineland-Palatinate)

RegE EEA	Entwurf eines […] Gesetzes zur Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen (Draft of the AICCM)
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RiVASt	Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (Guidelines on Relations with Foreign Countries in Criminal Law Matters)
SaarPolG	Saarländisches Polizeigesetz (Police law of Saarland)
SK-StPO	Systematischer Kommentar zur Strafprozessordnung (legal commentary)
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung Sachsen-Anhalt (Police law of Saxony-Anhalt)
SOG M-V	Gesetz über die öffentliche Sicherheit und Ordnung Mecklenburg-Vorpommern (Police law of Mecklenburg-Western Pomerania)
StGB	Strafgesetzbuch (Penal Code)
StPO	Strafprozessordnung (German Code of Criminal Procedure)
StraFo	StrafverteidigerForum (law journal)
StV	Strafverteidiger (law journal)
ThürPAG	Polizeiaufgabengesetz Thüringen (Police law of Thuringia)
TKG	Telekommunikationsgesetz (Telecommunications Act)
TKÜV	Telekommunikations-Überwachungsverordnung (Telecommunications Interceptions Ordinance)
TR TKÜV	Technische Richtlinie TKÜV (Technical Directive TKÜV)
VoIP	Voice over IP
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik (online law journal)
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft (law journal)
ZUM-RD	Zeitschrift für Urheber- und Medienrecht – Rechtsprechungsdienst (law journal)

Hungary*

National Rapporteur:
Katalin Parti

* This report reflects legislation and case law as of April 2019.

Contents

I. Security Architecture and the Interception of Telecommunications

A. Law Enforcement Institutions and Security Services with Powers of Telecommunications Interception

1. National security architecture

The relationship between secret surveillance for law enforcement and civil/national security purposes

Secret surveillance for law enforcement and civil/national security purposes are regulated in Hungary partly by the Act on Criminal Proceedings and partly by police and state security legislation. The regime is twofold: interception instruments are used on the one hand for law enforcement purposes, and on the other for constitutional protection (state security) purposes.

– *Interception for intelligence purposes*

The civil secret services charged with protecting national security interests may use intelligence instruments for the purposes of protecting the Constitution, sovereignty, and national security. These include: the Office for Constitutional Protection *(Alkotmányvédelmi Hivatal)*, the Information Office *(Információs Hivatal)*, the Military State Security Service *(Katonai Nemzetbiztonsági Szolgálat)*, the Anti-Terror Information and Criminal Analysis Centre *(Terrorelhárítási Információs és Bűnügyi Elemző Központ)*, and the National Security Special Service (NSSS) *(Nemzetbiztonsági Szakszolgálat)* – the latter being the body tasked with gathering secret information for national security purposes (Act CXXV of 1995 on national security services, hereinafter NSSA, Section 1 Points a–e)). The duties of bodies in charge of national security include gathering foreign information important for governing, gathering information necessary for national defence, and covert surveillance using secret service methods to avert threats against Hungary.

The executing body (NSSS) is separate from the organisations with legal competence to ensure the latter have control over the execution.

– *Interception for law enforcement purposes*

Secret surveillance for law enforcement purposes ("secret intelligence," i.e., intelligence outside of criminal proceedings) is used to prevent and investigate crimes, to establish the identity of the perpetrator, and also to apprehend them. Un-

der legislation in effect up to 1 July 2018[1] this had two areas: secret information gathering (SIG) and secret data interception (SDI). Secret information gathering could be used *before* criminal investigations were ordered, while secret data interception could only be used following the order of investigations, as part of the criminal proceedings (secret intelligence). The name of the two legal instruments was misleading; they were not differentiated by the type of information that could be gathered (i.e., information or only data), but whether they took place *before or after* the initiation of criminal proceedings.

The Counter-Terrorism Centre *(Terror-elhárítási Központ)* is also an investigative authority; it is an organisation granted law enforcement competence in the Act XXXIV of 1994 on the Police Forces (hereinafter Police Act), but it also took over certain counter-terrorism functions from bodies in charge of national security. Although it is considered a police authority, it can perform secret information gathering like the NSSS – it is entitled to both order and execute such information gathering. This was the method of gathering secret information which was challenged in the case of *Szabó and Vissy v. Hungary* at the European Court of Human Rights (ECtHR) in Strasbourg.[2] Their submission notes that the judiciary must give permission for secret information gathering, yet such information gathering for defence purposes carried out by the Counter-Terrorism Centre needs only the permission of a minister. The European Court of Human Rights is of the opinion that experimental, non-targeted, secret information gathering of an explorative nature – that was transferred to the Counter-Terrorism Centre, and is subject to ministerial permission – infringes on the rights to private life, communication, and informational self-determination stipulated in Articles 8 and 10 of the European Convention on Human Rights. The ECtHR upheld Szabó and Vissy's submissions and ruled that judicial permission would be required for such surveillance rather than ministerial permission.[3]

2. Powers for the interception of telecommunication

a) Authorising powers

Authorising powers, such as those under the current system of secret surveillance, are very complex. If civil secret services engage in intelligence activities, the use of the given instrument (e.g., data interception) is authorised by the Minister of Justice, as this is a government competence. If the secret surveillance is performed for law enforcement purposes, it has to be authorised by a court. If the police or the National Tax and Customs Administration uses secret surveillance for law en-

---

[1] The currently effective Act XC of 2017 on Criminal Proceedings replaced Act XIX of 1998 (on Criminal Proceedings) 1 July 2018.

[2] *Szabó and Vissy v. Hungary* (Application no. 37138/14).

[3] *Szabó and Vissy v. Hungary, ibid*.

forcement purposes, it has to be authorised by the minister in charge of justice. A secret instrument preceding an order for the investigation is typically the use of prison agents or investigators. If the secret surveillance takes place after the investigation is ordered, it has to be authorised by the judge in charge of the investigation.

b) Provisions of the new Criminal Proceedings Act on surveillance

Act XC of 2017 on Criminal Proceedings (hereinafter new CP) which entered into force on 1 July 2018 clarified this system considerably. It stipulates that all activities, which were previously conducted as part of SIG or SDI by the prosecutor's office / investigative authority, are *covert instruments* of the criminal proceedings, subject to the authorisation of the judge in charge of the investigation. Even though the distinction between secret surveillance ordered before and after the investigation remains, these are always subject to a judge's authorisation, and require the authorisation of the same judge. (The old Criminal Proceedings Act effective until 30 June 2018 stipulated that the SIG and SDI were subject to authorisations from judges in different areas. SDI could be ordered by the judge in charge of the investigation, while SIG was subject to the authorisation of a judge appointed by the president of the given county's tribunal.) Evidence gathered during surveillance ordered for law enforcement purposes has to be admissible in the criminal trial. This is also clarified in the new CP: it bypasses and solves the problem of data acquired with different methods by different authorities, under different authorisations potentially not admitted as evidence in criminal court proceedings. The new CP does not however expressly stipulate that national security services cannot engage in criminal intelligence activities. However, it does stipulate that the prosecutor (who is in control of the investigation) has to be informed about the use of all secret intelligence instruments for law enforcement purposes. Under the supervision of the prosecutor, the type of data, and the manner of data acquisition and recording will be acceptable to allow the data to be used in criminal proceedings.

– *Case #1*

Up until 1 July 2018, there were many cases in practice where during secret surveillance for national security purposes data was gathered about the person observed, which pointed to a crime. However, data acquired in secret surveillance for national security purposes could only be made admissible in criminal proceedings through a complicated procedure, as it was not acquired through activities giving rise to criminal proceedings, nor with the authorisation of a judge, but rather the Minister of Justice. In such cases, the intelligence work had to be authorised again by the judge. In cases where the data had already been acquired as a result of the surveillance, a second authorisation only was possible if the surveillance was conducted under the authorisation of the Minister of Justice, and was indicative of ac-

tivities, which would have merited secret intelligence measures as part of criminal proceedings. Even in these cases, the data could be used as evidence in the criminal court if the criminal report was made to the police immediately after gathering the data, and the investigation was immediately ordered.

The Hungarian Civil Liberties Union (HCLU)[4] is of the opinion that all secret intelligence measures should only be ordered legally with a judge's authorisation.[5] Transparency International (TI)[6] says however that if the secret services conduct intelligence measures for the purposes of constitutional protection, a criminal judge should not take responsibility for them, as by definition the secret services are in violation of Hungarian law gathering information outside of a criminal procedure.[7] A judge should not give authorisation for measures taken for constitutional protection, as secret surveillance conducted by secret services does not serve any law enforcement goal, and rather involves political responsibility. The Hungarian government should therefore take responsibility for them, meaning it is the Minister of Justice who should authorise such actions.

– *Case #2*

In 2016 Szabó and Vissy took a case to the ECtHR[8] based on their objection to an act from 2012 and one from 1995. Under the act on national security agencies, which came into force in 1995, these services could carry out secret surveillance for the purpose of national security without the authorisation of a judge, but from the Minister of Justice. In this case, Máté Szabó, together with former data privacy commissioner László Majtényi, and lawyer Beatrix Vissy objected to the fact that courts practice no actual control over secret intelligence activities, which results in the unconstitutional situation, where the observation of citizens is an internal affair of the government. After the Hungarian Constitutional Court's rejection of this case in 2013 they took it to the ECtHR, which upheld their submissions in 2016. The ECtHR was of the opinion that Hungarian legislation is in violation of the fundamental human right to respect for private life enshrined in the European Convention on Human Rights. Yet the court ruled that there are exceptions from this, such as measures taken to protect national security interests, public safety, the economic welfare of the country, or to prevent riots or crimes. But Szabó and Vissy actually did not contest whether the State has the right to limit the rights of its citizens to achieve certain goals such as the safety of its citizens. Their concern was the fact

---

[4] The Hungarian Civil Liberties Union is a human rights NGO. Website available in Hungarian: https://tasz.hu

[5] HCLU, interview.

[6] Website of Transparency International Hungary, available also in English: https://transparency.hu/en/

[7] TI, interview.

[8] *Szabó and Vissy v. Hungary*, (n 2).

that this limitation is not subject to any control in Hungary. The ECtHR ruled in response that there are certain cases, where it would cause disproportionate delay to wait for a court decision, and in such cases an exception can be made, and the surveillance can be conducted without prior authorisation, but in such cases the lawfulness of the decision must be reviewed by a court at a later date. However, there is no such opportunity in Hungary, neither at the time of the case, nor at the time of writing.

c) The overlap of plea agreements for law enforcement and national security purposes in the Criminal Proceedings Act

Law enforcement and national security competences overlap in Hungarian legislation on criminal proceedings (Act XC of 2017 on the Criminal Procedure, effective as of 1 July 2018) in so far as the act stipulates that the public prosecutor may enter a plea agreement not only for law enforcement reasons, but also in the interest of national security, as stipulated in the NSSA. This means that if a concerted cyberattack against Hungary has to be prevented, investigated, or uncovered, i.e., a political attack is about to begin against the political interests of the Hungarian government, a plea agreement may be concluded and less serious crimes – e.g., online paedophilia, illegal organisation of online gambling – may be waived, so that national security interests are not compromised.

B. Statistics on Telecommunications Interception

1. Obligation to collect statistics

In accordance with Article 10 of the data retention directive (DRD) of the European Parliament and the Council,[9] Member States were obliged to create a public statistical database. However, the DRD never entered into effect, therefore the database was not created in Hungary. To ensure the control of the implementation of the directive and to test the efficiency of the procedure it stipulates, the European Commission also ruled that Member States should provide data annually to the Commission about the number of instances where electronic data was handed over based on the DRD for the purposes of national security or criminal proceedings. The Commission only published an evaluation report[10] in 2011, years after the directive entered into force on 3 May 2006, but Hungary did not provide data for the

[9] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[10] https://edps.europa.eu/data-protection/our-work/publications/opinions/evaluation-report-commission-council-and-european_en

report.[11] It has to be noted that despite this, several other provisions of the directive were transposed into Hungarian legislation. The transposition involved the obligation of providers of services in relation to e-commerce and electronic communication to collect certain metadata (traffic data, subscriber data), and content data, and to hand this over to the authorities for law enforcement and national security purposes. Providers of electronic communications services have to respond to requests from law enforcement authorities and provide the data requested if there is a valid legal basis of such requests. Certain internet service providers – the largest service providers in Hungary – publish their law enforcement reports (Telenor, Vodafone, Magyar Telekom as part of Deutsche Telekom).[12] Telecommunications service providers maintain their own database on requests from the authorities competent to make requests. This encompasses about 40,000 (+/-2,000) data requests per year, but one data request may actually involve the data of several users.[13]

Even though service providers do maintain statistics on data requests for law enforcement purposes (data handover log), it is not based on the number of requests, but rather the number of times data was handed over within a year. This however does not contain a breakdown of the requests by authority, for which reason it is not possible to distinguish between requests for law enforcement, national security or military purposes. However, there does exist breakdowns by IP address (for Magyar Telekom 8,752 individual ones in 2017), by subscriber master data (for Magyar Telekom 34,092 in 2017), and by traffic data / metadata (e.g., call lists) (for Magyar Telekom 77,589 in 2017).[14] The service providers also maintain a data provision log, with which they can prove in criminal proceedings that the authority gained access to the data used as evidence in the case through a request to the service provider. No statistics are maintained on (classified) data requests for national security purposes.[15]

---

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52011DC0225

[12] Telenor: https://www.telenor.com/wp-content/uploads/2015/05/Authority-Requests-Access-Report_2016.pdf; p. 6.

Vodafone: https://www.vodafone.com/content/dam/vodafone-images/sustainability/drf/pdf/vodafone_drf_law_enforcement_disclosure_country_demands_2015-6.pdf; p. 10.

http://www.vodafone.com/content/dam/vodafone-images/sustainability/drf/pdf/vodafone_drf_law_enforcement_disclosure_legal_annexe_2016.pdf; p. 58.

Magyar Telekom (part of Deutsche Telekom): https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/transparency-report-363546

[13] Telecommunications service providers, interviews.

[14] See the public transparency report of Deutsche Telekom.

[15] Telecommunications service providers, interviews.

2. Non-public database for national security purposes

Under the NSSA, the NSSS – i.e., the executing organ of secret information gathering ordered by bodies authorised to conduct secret information gathering for national security purposes – maintains a database about the tasks of the service provider, which contains (Section 61 Paragraph (3) of the NSSA) a) the written request of the ordering organisation with the necessary authorisation, b) the personal data required to identify the person specified in the request, c) the description of the instruments and methods of secret information gathering and secret data interception used in the case, and other information and technical data of non-personal nature, and d) the register of data carriers forwarded to the ordering organisation. This data however cannot be made public even after the procedures are concluded.

II. Principles of Telecommunications Interception in Constitutional and Criminal Procedural Law

A. Constitutional Safeguards of Telecommunications

1. Areas of constitutional protection

a) Legislative and other legal guarantees against data stockpiling

The right to privacy, the right to respect for private and family life, and the closely related right of informational self-determination are stipulated in Article VI of the Fundamental Law of Hungary.[16] These rights, which are closely linked to human dignity, are intended to jointly ensure that the privacy of a person may not be invaded against their will. At the same time the limitation of the right to privacy is also accepted in constitutional democracies for legitimate purposes such as national security and public safety, the prevention and investigation of crimes, and meeting the State's need for criminal prosecution. However, the limitation of the right to privacy has to pass several instances of fundamental rights proofing as regards the constitutional admissibility of the infringement of fundamental rights ("three-tiered constitutionality test").

First, the limitation has to be suitable to achieve the desired goal (suitability test). Second, the requirement for necessity may only be met if the planned limitations of rights are inevitably demanded by the abovementioned goals, i.e., there is a qualified threat, in relation to which the available instruments would not be sufficient (test of necessity). Third, the proportionality of the planned limitations depends on the constitutional guarantees observed (proportionality test). Even if con-

---

[16] Fundamental Law of Hungary, 25 April, 2011.

ditions exist under which a limitation of rights is suitable and necessary, it is only possible in a strictly regulated and transparent legal procedure, and with adequate institutional guarantees covering all elements of the conditions meriting an interference in privacy. "No considerations of expedience or equitableness may justify the disregard for the guarantees protecting the freedom of individuals in a state of law."[17] The above draft laws referred to in Section I.A. of this report which limit fundamental rights would have had to be made public in the interest of a transparent societal debate – based on Act CXXXI of 2010 on public participation in the preparation of legal regulations –, but according to HCLU, this did not happen.[18]

The Constitutional Court has yet to decide on the changes in legislation motivated by the fight against terrorism, but HCLU has already filed separately for each of the drafts to be declared unconstitutional. An authorisation from judges would guarantee that these safeguards are observed. Without knowing the statistics, it is impossible to see how many requests were rejected and on what grounds by the courts. Only in the knowledge of such statistics would it be possible to say that these judicial safeguards are observed.

b) The Fundamental Law of Hungary (25 April 2011)

Article I Paragraph (3)

The rules for fundamental rights and obligations shall be laid down in an Act. A fundamental right may only be restricted to allow the effective use of another fundamental right or to protect a constitutional value, to the extent absolutely necessary, proportionate to the objective pursued and with full respect for the essential content of such fundamental right.

The Fundamental Law stipulates the right to respect for private life (Article VI Paragraph (1)), the right to the protection of personal data and the right to access data of public interest (Article VI Paragraph (2)), and also that the application of the right to the protection of personal data and to access data of public interest has to be supervised by an independent authority established by a so called cardinal Act adopted with a two-thirds majority of all Members of the [Hungarian] Parlament [hereinafter MPs] (Article VI Paragraph (3)).

The requirement of purpose limitation (proportionality, necessity, suitability) is enshrined in specific legislation stipulating the competences of the given body. The specific Acts mentioned below determine the scope and approach under which such instruments can be used.

---

[17] HCLU, interview.

[18] HCLU, A Társaság a Szabadságjogokért álláspontja a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló törvény tervezetéről, 2016, available at https://tasz.hu/files/tasz/imce/a_tasz_allaspontja_a_terrorizmus_elleni_fellepessel_osszefuggo_egyes_torvenyek_modositasarol_szolo_torveny_tervezeterol.pdf

2. Specific legislation and safeguards

a) Act CXXV of 1995 on the National Security Services (NSSA)

Section 39 Paragraph (2) NSSA

In the context of their data management activity, the National Security Services shall use that instrument which is absolutely necessary to achieve the given objective and which least restricts the individual rights of the person concerned.

This Act stipulates that national security services are under the supervision of the National Security Committee of the Parliament, which is always chaired by an MPs from the opposition (Section 14 NSSA). As part of its parliamentary supervision activities, the Committee among other things also reviews complaints regarding the unlawful activities of national security services – although they have a right to do so, there is no such obligation (Section 14 Paragraph (4) Point c) NSSA), and if they establish unlawful or unintended activities, it may call on the Minister of the Interior to take the necessary measures, may initiate an inquiry into those responsible, and the Minister informs the Committee about the findings of the inquiry (Section 14 Paragraph (4) Point f NSSA).

National security services may conduct secret information gathering. They are only allowed to use the special instruments and methods of secret information gathering if data necessary for performing their tasks stipulated in legislation is not available in any other way (Section 53 Paragraph (2) NSSA). The secret information gathering – subject to an authorisation – is authorised by a judge appointed by the president of the Municipal Tribunal of Budapest (Fővárosi Törvényszék), and in some cases by the Minister of Justice. The request also has to contain the reasoning for the necessity of the secret information gathering (Section 57 Paragraph (2) NSSA). The authorisation may be granted for a maximum of 90 days, and may be extended once by a further 90 days in justified cases (Section 58 Paragraph (4) NSSA), i.e., it may be valid for 180 days.

Secret information gathering subject to an external authorisation has to be immediately terminated when it reaches the goal specified in the authorisation, or becomes for any reason unlawful (Section 60 Paragraph (1) NSSA). In the latter case, the data gathered in the process has to be destroyed with immediate effect (Section 59 Paragraph (2) NSSA).

b) Act on Criminal Proceedings (CP Act)

The new CP Act stipulates conditions for necessity in relation to accessing the personal data of the individual concerned in the procedure and the files of the case, the limitations on informing the public, the scope of facts to be established in evidence of the charge, and the manner of use of the listed investigative activities.

The CP Acts also provide guarantees for the protection of fundamental rights in relation to the use of coercive measures with the potential to infringe fundamental rights. An example of this is in relation to the order for the preservation of data recorded by way of a computer system (Section 158/A old CP Act; and Section 315 new CP Act).[19] The court, the public prosecutor or the investigative authority orders the preservation of data recorded by way of a computer system, which is itself evidence, or is necessary for establishing data evidence, or the identity and whereabouts of the suspect. The aim of this legal instrument is to avoid seizure, which in many cases – where large IT systems are involved – would result in a disproportionately significant limitation of the rights of the person under surveillance. The entity ordered to preserve the data is obliged to preserve unchanged the data recorded by way of a computer system stipulated in the authorisation from the time he was informed of the order, and has to provide for its safe storage, if necessary separate from other data. Following the order for data preservation, the investigative authority immediately begins the analysis of the data concerned. Depending on the result of this, the seizure of the data in the form of copying into an IT system or onto a data carrier is ordered, or the order for data preservation has to be lifted. The obligation to preserve data expires upon the seizure of the data, but no longer than three months.

c) Act XXXIV of 1994 on the Police Forces (Police Act)

The Police Act stipulates necessity and purpose limitation criteria for investigative measures and data management – including the implementation of crime prevention, intelligence and law enforcement activities (Section 77 Paragraphs (1) and (2) Police Act). The scope of data necessary to perform police duties, i.e., the scope of the "data to be managed" is stipulated under Sections 81 to 91/T.

The head of the data management body of the police has to ensure that in the interest of protecting personal data, the person under investigation is informed of the scope of their data managed by the police, and that they can exercise their right to corrections, deletion and blocking in a manner stipulated in the Act CXII of 2012 on informational self-determination and the freedom of information (Info Act). The person concerned may request that his stored data is deleted, if the management of such data is unlawful, or the period of storage stipulated in legislation has expired, or the deletion of the data was ordered by a court or the National Authority for Data Protection and Freedom of Information *(Nemzeti Adatvédelmi és Információszabadság Hatóság)* (Section 80 Paragraph (2) Police Act). The person concerned may turn to a court or the National Authority for Data Protection and Freedom of In-

---

[19] While the old CP Act stipulated the preservation of data stored in an IT system, the new CP Act, entered into force on 1 July 2018 stipulates the order for the preservation of *electronic data*. The provision is otherwise unchanged.

formation in case of an infringement of his rights, of which he must be informed (Section 80 Paragraph (4) Police Act).

If a person's fundamental rights were infringed by an action of the police, they may also make a complaint to the police body, which took the given action, and may request that their complaint is reviewed by the head of the organisation exercising supervision over the police body (e.g., Commander in Chief of the Police, the Director General of an anti-terror organisation, etc.), which conducted the action concerned and against which the complaint is made (Section 92 Paragraph (1) Police Act).

d) Act CXXII of 2010 on the National Tax and Customs Administration (Tax Authority Act)

We discuss the Tax Authority Act in this report, because the investigative authority of the National Tax and Customs Administration also conducts law enforcement, crime prevention, intelligence and investigative activities (Section 35 Tax Authority Act). Coercive measures infringing the rights of individuals may only be taken if necessity and proportionality requirements are met (Section 36/E Tax Authority Act). The National Tax and Customs Administration may conduct secret information gathering for law enforcement purposes in relation to serious crimes (money laundering and financing of terrorism) whether or not a judicial authorisation is required, and also in relation to other crimes delegated to its competence as an investigative authority, which are committed on a commercial scale or in a criminal association, are punishable with imprisonment of up to three years, and violate tax regulations (Section 63 Paragraph (1) Tax Authority Act).

As part of its secret information gathering activities subject to judicial authorisation, the National Tax and Customs Administration may e.g., have access to the contents of communications transmitted by way of an electronic communications service, may record the content with technical solutions, and may have access to, record and use data stored on or transmitted by way of computer system (Section 63 Paragraph (1) Point e–d) Tax Authority Act).

The data acquired in such proceedings related to persons not targeted by the proceedings has to be destroyed immediately (Section 63 Paragraph (2) Tax Authority Act). The National Tax and Customs Administration, like any authority entitled to conduct secret information gathering subject to judicial authorisation, delegates the use of the so called "special instruments" to the NSSS (Section 63 Paragraph (5) Tax Authority Act). The use of such instruments may only be ordered for a maximum 90 days, which may be extended by an additional 90 days upon request (Section 63 Paragraph (6) Tax Authority Act). If authorising the use of a special instrument would result in a delay which would be contrary to the interests of a successful law enforcement action, the head of the NSSS may authorise the use of the special instrument until the judge can reach a decision, on condition that if the

judge does not grant an authorisation, or if the goal stipulated in the authorisation is achieved, the use of the instrument has to be terminated with immediate effect (Section 65 Tax Authority Act). Data acquired by way of using a special instrument has to be destroyed within eight days following the end of surveillance, if it is not relevant for the goal of the surveillance activities, or is related to a person not involved in the case.

The provisions on data management, databases, data provision, handover and receipt are included in Sections 66 to 80/A of the Tax Authority Act. Within that, data management for law enforcement purposes is governed by separate provisions. Such data may only be used for law enforcement purposes (purpose limitation) (Section 69 Paragraph (1) Tax Authority Act). The investigative authority of the National Tax and Customs Administration may gather data from law enforcement databases (e.g., the shared electronic database of the police and the public prosecutor's office called "Robocop" *(Robotzsaru)*) (Section 73 Paragraph (5) Tax Authority Act). Purpose limitation also applies here. Data considered to be a tax secret or customs secret may only be taken over from other databases with the authorisation of a public prosecutor.

For the purposes of law enforcement, the investigative authority of the National Tax and Customs Administration may forward personal data and law enforcement data to other Member States of the European Union, and to international organisations and data management systems created by a legal act of the European Union, and may also receive data from them in accordance with a legal act of the European Union or a bilateral or multilateral international treaty within the content scope and period stipulated therein. Personal or law enforcement data managed by the investigative authority of the National Tax and Customs Administration may only be handed over to third countries and international organisations for law enforcement purposes in accordance with an international treaty in the content scope and period stipulated therein, if criteria stipulated in the Info Act are met, and if the competence of the receiving authority of the third country or the receiving international organisation includes the prevention, investigation, and detection of crimes, conducting criminal proceedings or implementing criminal sanctions (Section 77 Paragraphs (1 to 2) Tax Authority Act). If it is established at a later date that inaccurate data was forwarded or data was forwarded unlawfully, the receiver of the data has to be informed of this immediately. In accordance with the Info Act, a data transmission log has to be kept of all data transmissions performed through international cooperation in criminal matters (Section 77 Paragraph (4) Tax Authority Act). This log is not public, and it was therefore not possible to request data from it for this country report.

e) Regulations applicable to internet and telecommunications service providers

Regulations on internet and telecommunications services also stipulate a purpose limitation fpr data management. In accordance with the act on electronic commercial services (Act CVIII of 2001; E-Commerce Act), for the drafting of contracts, determination and modification of their contents, the monitoring of their performance, the invoicing of fees from the contracts, and the collection of receivables arising from such, and also for the provision of the given services the service provider may manage data needed and sufficient for the identification of the customer (Section 13/A E-Commerce Act). The "principle of data efficiency" means in relation to the obligation of electronic service providers that they have to select the instruments used in the course of providing services related to the information society in a manner which ensures that personal data is only managed, if it is absolutely necessary for the provision of the service, and even so only in the scope and for the period necessary.[20] The data managed for the purposes of the service has to be deleted immediately if the contract is not concluded or terminated, and when invoicing stops. In addition to the notification stipulated in Sections 14 to 19 of the Info Act, the service provider has to ensure that before the service starts and during the service customers have the opportunity to be informed as to what data files the service provider is managing, including data not directly linked to the customer.[21]

f) The Civil Code (Act V of 2013)

The Cicil Code stipulates the rights to private life and the freedom of information as personal rights related to one's own images, sound recordings, and data (Section 02:43 Civil Code).

3. Consequences if these safeguards are not complied with

If the data gathering is performed in breach of regulations, the data thereby acquired may not be submitted as evidence in criminal proceedings or in any other proceedings.

In addition, an entity managing data without authorisation typically commits the crimes of unauthorised secret information gathering or data acquisition (Section 307 Act C of 2012 on the Criminal Code), committed specifically by breaching regulations on secret data interception and secret information gathering; the crime of unlawful data acquisition (when, e.g., someone plants a covert listening device in a private residence for private purposes, and learns a private secret) (Sec-

---

[20] Mező, I., Személyes adatok védelme az Európai Unió jogában és Magyarországon, PhD értekezés, Miskolci Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskola, 2009, p. 286, available at http://midra.uni-miskolc.hu/document/5522

[21] *Ibid,* p. 287.

tion 422 Criminal Code); and an offence caused in the IT system or data (if e.g., the entity entitled to secret surveillance oversteps the boundary /goal, period, etc./ of their authorisation, and their access to the IT system under surveillance does not stop) (Section 423 Criminal Code).

4. Summary: Constitutional guarantees, checks and balances

The problem of Hungary's legal system not only lies in mass surveillance (gathering traffic data), but also in data preservation. There are no organisational, institutional or procedural guarantees in relation to data management. The case of *Szabó and Vissy v. Hungary* highlighted that when one of the executive state bodies (the Minister of Justice) further authorizes another executive state body to keep citizens under surveillance, it creates a constitutional problem, as all executive state bodies are guided by the same political will. In that particular case the ECtHR adopted a positive decision, and upheld the opinion of Szabó and Vissy. This should have encouraged the Hungarian legislator to take two steps: 1) create the legal foundations of an independent authorisation process in cases involving secret surveillance for national security purposes – Szabó is of the opinion that a court or the National Authority for Data Protection and Freedom of Information should authorise such procedures,[22] and 2) a legal regulation stipulates that the person under surveillance has to be informed when the surveillance procedure is concluded and the goal of surveillance and the goal of the operation is no longer at risk, for the purpose of legal remedy (as the "information compensation" for the secret surveillance). The decision of the ECtHR became final in autumn 2016, but the Hungarian legislator has not yet adopted any corresponding legislation.

This gives rise to the question of what happens if the legislator of a country is not moved to implement a given decision? There is a sanction for such cases, i.e., the payment of a compensation to the winning party stipulated in the ECtHR. This however does not necessarily put an end to the unconstitutional situation: "The Hungarian government usually pays the compensation [i.e., in cases where ECtHR renders it so], but they are not good at solving systematic problems."[23]

B. Powers in the Code of Criminal Procedure

The Acts on Criminal Proceedings (both the old and the new) link the use of coercive measures to "reasonable suspicion." It follows from this that the use of coercive measures may occur in the so called operative phase, which starts with the suspicion becoming known. Coercive measures may not be ordered again in rela-

---

22 Máté Szabó, interview.

23 Máté Szabó, interview.

tion to the same crime once they have been terminated. Coercive measures may be ordered and terminated by a court, a public prosecutor or an investigative authority.

Coercive measures are regulated by differentiated provisions in the Acts on Criminal Proceedings (old CP: Sections 126 to 159/A, new CP: Sections 271 to 338): "Coercive measures limiting personal freedoms may be important, and in certain cases essential instruments of successful criminal proceedings, but we also have to be aware of the fact that the provisions of legal regulations on criminal proceedings stipulate a restriction of fundamental rights. It applies to these norms of criminal procedural law CPCP in particular, that the greatest possible care must be taken when laying down norms, as the intersection of efficiency and due process – which varies from institute to institute – is particularly narrow in relation to coercive measures restricting personal freedoms."[24] The use of coercive measures is only admissible for the reasons and with a scope (rules of ordering and terminating such, expiry) specified in legislation. Under the new CP Act, coercive powers may be ordered subject to the following conditions:

– restricting the rights of the person targeted by the coercive measures only to the extent necessary (Section 271 Paragraph (1) new CP Act) and proportionate (Section 271 Paragraph (2) new CP Act) extent;
– the fairest possible treatment and respect for the fundamental rights of the person concerned (Section 271 Paragraph (3) new CP Act);
– disturbance of persons other than the person concerned only to the extent necessary (Section 271 Paragraph (3) new CP Act);
– respect for private life as far as possible (Section 271 Paragraphs (4) and (5) new CP Act) in a manner that guarantees circumstances not linked to the criminal proceedings are not made public;
– avoiding unnecessary damage (Section 271 Paragraph (6) new CP Act).

Beyond these, the new CP Act also stipulates further conditions for coercive measures limiting personal freedoms (Sections 276 to 278 new CP Act), which are as follows: Coercive measures limiting personal freedoms may be ordered by a judge upon the proposal of a public prosecutor, if:

– a procedure may only be ordered due to crimes punishable by imprisonment;
– the coercive powers may be ordered by a judge;
– in the case of reasonable suspicion or an indictment;
– ensuring the presence of the person concerned, or their escape or hiding, and the threat of this;
– making the evidence process more difficult or impossible, or a threat of this, including the intimidation or unlawful influencing of others to that end, or the de-

[24] Miskolczi, B., A kényszerintézkedések új rendszere, Jogász/Világ, 2017. február 21, available at https://jogaszvilag.hu/rovatok/szakma/a-kenyszerintezkedesek-uj-rendszere

struction, forgery, or hiding of physical evidence, electronic data, and assets to be confiscated, or the threat of this;
– preventing opportunities for repeat offending;
– preventing the continuation of the perpetration of the crime, or its threat;
– beyond these, it is important to keep the duration of coercive powers restricting personal freedoms at a minimum (Section 279 new CP Act).

III. Powers for Accessing Telecommunications Data in the Law of Criminal Procedure

A. Overview

1. Obligation to handover data in criminal proceedings

The cooperation obligation of electronic communications service providers in the handover of data in criminal proceedings is regulated by the CP Act (Section 244 Paragraph (6) new CP Act). The cooperation obligation also covers the service provider's obligation for decryption, if the encryption was performed by the service provider and not the user himself (Section 264 Paragraph (2) new CP Act). In addition to data requests for the purposes of criminal proceedings, there are also data requests for policing (crime prevention and detection) purposes (Section 68 Paragraph (1) Police Act) and for national security and defence purposes, which are regulated by a separate specific Act (Section 41 Paragraph (1) NSSA) and the Electronic Communications Act (Section 92 and Section 155 Paragraph (5) E-Communications Act). The cooperation obligation of the service provider in the criminal proceedings in relation to implementing the coercive measure of making electronic data temporarily inaccessible and the sanction of making electronic data permanently inaccessible (Section 158/A old CP Act; Section 335 new CP Act; Section 77 of the Criminal Code) is regulated in Section 92/A of the E-Communications Act. The detailed rules of the cooperation between service providers and the listed organisations for the purposes of criminal proceedings, crime detection and national security are found in Government Decree No. 180/2004.[25]

The Criminal Proceedings Act contains the list of bodies, which may request data from the service provider (Section 262 Paragraph (1) new CP Act). These include: the investigative authority and the internal body of the police for crime prevention and crime detection, and the counter-terrorism unit of the police. The new

[25] Government Decree No. 180/2004 (V.26.) Decree on the rules of cooperation on electronic communication organisations and organisations authorised to perform secret information gathering and secret data interception, hereinafter: Government Decree No. 180/2004.

CP Act stipulates that bodies entitled to request data from the organisations specified in the Act (e.g., electronic communications service providers) may only do so with the authorisation of the public prosecutor's office (Section 262 Paragraph (1) new CP Act). It is important to note here that according to the old CP Act effective until 30 June 2018, the investigative authority *did not require an authorisation* from a public prosecutor for data requests in public criminal proceedings. Both the investigative authority and the service providers gave voice to their scepticism as to whether the system of authorisations by public prosecutors stipulated by the new CP Act would be possible to implement without an undue increase in administration and the lead time of data transmissions.[26]

The scope of data, and the purpose and period of data gathering in relation to the obligation of electronic communications service providers for data preservation and transmission are stipulated in the E-Communications Act (Section 159/A E-Communications Act).

The bigger telecommunication service providers (Magyar Telekom, Vodafone, Pannon, Telenor, UPC) have to conclude an agreement with the police and the public prosecutor's office on cooperation for the purposes of crime prevention and law enforcement, and for the purposes of national security with the Ministry of the Interior, which stipulate in what form they can hand over data passing through their system, i.e., the conditions – as regards legal regulations and format – for meeting automated data requests (Government Decree no. 180/2004). The police and the secret services delegate liaison officers to telecommunications service providers. (These are secret agreements, which cannot be made public, and cannot be publicly referenced.)

The automatic (electronic) data transmission system was developed as part of the e-administration project for the National Tax and Customs Administration, Counter-Terrorism Centre, the National Police Headquarters, and the Budapest Police Headquarters. But not all authorities with investigative competences can submit electronic data requests for technical and organisational reasons. The public prosecutor's office has a direct interface to service providers, which enables the public prosecutors to initiate searches directly in the database of the service providers (this enables faster searches even more directly than the automatic data request system of the police – a.k.a. Robocop –, without filling in forms).

Before automatic data requests, approximately 50 members of staff were needed at the bigger service providers to sort out the data manually, and to meet the data requests received on paper or by fax. Today, in the age of automatic data requests, usually only an average of five members of staff are needed at a service provider to sort out the data for the requests. Automatic data requests are made possible by dedicated interfaces between the service providers and the National Police Head-

---

[26] Investigative authority, telecommunication service providers, interviews.

quarters. The police use this system through the Robocop network, where 20 to 30 data request templates are available. After filling in one of these, the data can be obtained from the system of the service provider. Searches as well as queries are automatic in this system, and require no human intervention from the telecommunications service provider.[27]

2. Additional general clauses

An example of an additional general clause is the authorisation of data requests by the public prosecutor, which is introduced by the new CP Act (Section 262 Paragraph (1) new CP Act). (No authorisation is required from the public prosecutor for the data requests of courts – Section 261 Paragraph (1) new CP Act.) The new CP Act introduces the clauses on necessity and proportionality (Section 264 Paragraph (4) new CP Act), and purpose limitation (Section 264 Paragraph (5) new CP Act), and also the obligation to delete data, if it is not linked to the purpose of the data request (Section 264 Paragraph (5) new CP Act). Under the new CP Act, the person concerned also needs to be informed about the data request, which may be postponed, if such notification would endanger the success of the criminal proceedings (Section 264 Paragraph (7) new CP Act). The service provider may inform only the person concerned of the fact and scope of the data request (Section 264 Paragraph (7) new CP Act).

B. Interception of Content Data

1. Statutory provision

Under the new CP Act, "electronic data" which is acquired not only by way of public proceedings, but also through the "secret surveillance of IT systems" can be recognised as evidence in criminal proceedings (new CP Act, Chapter XXXIII: Physical evidence). The subject of interception is therefore the "secret surveillance of an information technology system" (Section 231 Point a) new CP Act), which requires an authorisation from a judge in each case. The new CP Act gives a definition of electronic data in Section 205: "Electronic data shall mean a representation of facts, information or ideas in any form, which is suitable for processing in an information technology system, including any application, which ensures the execution of certain functions in the information technology system. Unless otherwise stipulated in this Act, where this Act refers to physical evidence, it shall be understood to also include electronic data."

---

[27] Telecommunications service providers, investigative authority, interviews.

2. Scope of application

a) Contents of traffic covered by the respective provisions

Bodies authorised by the Police Act may as part of their crime prevention activities, with a judge's authorisation have access to the contents of communication transmitted through an electronic communications service, may record the accessed contents with technical solutions, and "may have access to, record, and use data stored on or transmitted by way of an information technology tool or system" (Section 69 Paragraph (1) Points d) and e) Police Act). Bodies authorised by the NSSA as part of their national security activities, with an external authorisation "may have access to the contents of communication transmitted through an electronic communication service, may record the accessed contents with technical solutions, and may have access to, record, and use data stored on or transmitted by way of an information technology tool or system" (Section 56 Paragraph Points d) and e) NSSA).

As we see, admissible access to the content of a communication transmitted through a communications network is not defined in legislation in a restrictive manner, but rather as a framework rule. The access may take any form , i.e., any type of electronic communication can be intercepted. The electronic communications service provider has to ensure the conditions of use of the tools and methods used to access messages and comments transmitted in an electronic communications network and data managed by the service provider by way of secret information gathering or secret data interception (Section 92 Paragraph (4) E-Communications Act), and have to install a sub-system for monitoring, for which the technical specifications are provided by the executing body of the interception, the NSS (Section 92 Paragraph (5) E-Communications Act). These technical specifications may refer to any type of data and any service or any type of communication. Government Decree No. 180/2004 gives a broad definition of communication: "content of communication: analogue or digital signals transmitted during communication and carrying speech or non-speech information (with the exception of accompanying information) independent of its format" (Section 2 Point b) Government Decree No. 180/2004). It is therefore possible to intercept person-to-person IP-based communications, communications transmitted on analogue lines, communications between a person and an automated information system, IP-traffic between a person's computer and their data storage in a cloud or other remote storage system, or IP-traffic between two independent computer systems. In conclusion, the Government Decree authorises the interception of any communication transmitted through electronic communications services. However, the specific types of communications, channels, and monitoring sub-systems currently in operation are not publicly known since not only the content and type of the intercept-

ed information is considered classified, but also the technical means used for the interception.[28]

One area which still does not work in practice is the interception of fifth generation computer data.[29] The technical specifications required for the interception of such data are under development. Until the NSS completes their development project, and orders service providers to install a corresponding sub-system, such data cannot be intercepted.[30]

b) Provisions for content interception

Section 159/A E-Communications Act stipulates what data electronic communication service providers must hand over under their data preservation obligation for law enforcement, national security, and defence purposes. The service provider is not obliged to hand over the *content* data of the communication, as they are not entitled to manage it (Section 157 E-Communications Act), therefore the content of communications may only be recorded by way of real-time interception, as part of a secret information gathering operation. The service provider may only store the content of the communications as long as it is essential for the provision of services and invoicing (Section 157 Paragraph (2) E-Communications Act). The SMS and voice mail accounts related to a mobile phone service, and email accounts, represent special cases as the service provider ensures storage capacities for them. In these cases, the provision of services requires that the content of the communications be stored for some time. The content of delivered and opened emails can be established during open investigations, while the content of emails not delivered can be discovered by way of secret information gathering (interception), and the content of emails delivered but not opened can only be captured with the authorisation of a public prosecutor.

c) Discussion on the constitutional requirements

In the case *Szabó and Vissy v. Hungary*, the plaintiffs contested the regulations on data gathering for national security purposes, but not data gathering for the purposes of criminal procedure. According to their submission (and the adopted decision), surveillance by national security services is problematic,[31] because the underlying legal regulations pertaining to these bodies stipulate that surveillance is

---

[28] Communications service provider, interview.

[29] These, e.g., include optical computers, which do not use electric signals but rather much faster light signals to carry the information. The research of quantum computers is also ongoing.

[30] Communications service provider, interview.

[31] *Szabó and Vissy v. Hungary*, (n 2).

subject to a minister's authorisation, and ministers are not independent of the government.

3. Special protection of confidential communications content

a) Protection of classified data in criminal procedure

According to the CP Acts, those under obligations of confidentiality cannot be forced to testify on classified data (Section 170 Paragraph (1) Point d) new CP Act). Based on sectorial Act CLV of 2009 on classified data (Classified Data Act), the classifier of data shall decide whether to grant the exemption or uphold the confidentiality obligation upon request by the court, the prosecution or the investigative authority. Otherwise, the CP Acts contain general rules for gathering information through covert means (Section 231 Point e) new CP Act).

b) Attorney's activities and legal services

The activities of attorneys and legal services are governed by Act LXXVIII of 2017 on the Activities of Attorneys (Attorney's Act). Title 7-8 provides details on professional secrecy, confidentiality obligations, and on the rights of authorities regarding documents containing information falling under attorney-client privilege (ACP).

As regards secrecy and confidentiality in attorney and client relations, "Every such communication shall fall under ACP, which consists of or includes facts, information or data that became known to the practitioner of legal services (attorney) in the course of providing such services. Unless otherwise provided by this law, practitioners of private legal services (attorneys) shall keep privileged information, including all documents and media containing such data, falling under ACP confidential. Practitioners of legal services shall refuse to testify or the disclosure of data regarding privileged information under ACP in any judicial or administrative proceedings, except if exempted from under this obligation by the holder of the privilege, who is entitled to dispose of the privilege, provided that no such authorization or exemption can be validly given from under the privilege in terms of data that became known to the practitioner acting as defence counsel" (Title 7 Section 9 Paragraph (1–3) Attorney's Act).

Powers of the authorities regarding documents containing privileged information under ACP and the protection of documents prepared for the purpose of the defence are also discussed in the Attorney's Act: "In the case of supervision, observation or search by any authority of such persons that are obliged by ACP, they shall not disclose information protected by ACP (incl. documents and data), and they shall not be obliged to provide witness testimonies or to disclose data. However, they shall refrain from obstructing the authorities. […]" (Title 8 Section 13 Para-

graph (1) Attorney's Act). "Authorities are entitled to look into such documents – without prejudice to the rights protected under this § and to an extent absolutely necessary in order to ascertain whether any reference to the quality of such documents as ones produced for the purpose of defence are manifestly ill-founded or not. If the classification of such documents is in dispute between the client and the authority, the authorities then may take the documents in dispute into their possession at the time of the observation or search provided that they are placed in such a container device, which prevents the data from being accessed or subsequently changed. As for the question of the classification of the document, upon the request of the authority, courts having jurisdiction in administrative proceedings shall decide in non-litigious proceedings with the hearing of the client in question. These documents are attached to the claim filed by the authority. If the court concludes that the documents do not qualify as ones produced for the purpose of defence, these shall be opened to the authorities. In cases to the contrary, the documents shall be transferred back to the client" (Title 8 Section 13 Paragraph (4–6) Attorney's Act).

c) Specific areas of protected data

Act XLVII of 1997 on the managing and protecting of health-related personal data contains rules on the protection of health-care data. Chapters 1 and 2 define the purpose of protection and definitions and the relevant rules specific to the area.

Communication is protected specifically under the law regulating financial and banking secrecy. The primary source of regulation of financial and banking secrecy is Act LXXV of 2007 on auditing services, which is often read together with Act LIII of 2017 against money laundering, generally breaking privilege into many sectorial fields and guarantees, in the interests of crime prevention.

Furthermore, the CP Act contains general data protection rules regarding the admissibility of data linked to private life (Section 231 Point e) new CPC Act).

d) Communication in a "core area of private life"

The general constitutional protection of privacy is stipulated by the Fundamental Law according to which "(1) Everyone shall have the right to have his or her private and family life, home, communications and good reputation respected. (2) Everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest. (3) The application of the right to the protection of personal data and to access data of public interest shall be supervised by an independent authority established by a cardinal Act" (Art. VI Paragraph (1)–(3) Fundamental Law).

There is no regulation available on the protection of the "core area of private life," but private secrets and correspondence are protected generally under the Act V of 2013 on the Civil Code (Sections 02:42–02:54 Civil Code).

In civil procedure (Act CXXX of 2016 on the civil procedure, in force since 1 January 2018) there are provisions regarding the inadmissibility of evidence obtained unlawfully, e.g., in violation of personality (privacy) rights, during civil procedure (Sections 269–270 Civil Procedure Act).

Sectorial legislation also can provide rules for protecting privacy rights, such as, e.g., Act CCXL of 2013 on the execution of penalties and measures, according to which prisoners' privacy rights must be respected (Section 119).

e) Access to classified information

The rules of the classification procedure and the levels and criteria of data classification are regulated in Hungary by Act CLV of 2009 on the protection of classified data (Classified Data Act). Classified data can be accessed in the same way as normal data, but access is only granted subject to a judge's authorisation. If, however, the classified data comes from a person whose testimony does not qualify as evidence, the data will have to be subsequently excluded from evidence.

It is always the judge that makes determinations under the relevant rules of criminal procedure for all modalities of data interception, the stage at which the interception takes place and in what way these privileges and/or the analysis of the respective captured information has to be conducted.

f) Discussion on the respective constitutional requirements

The right to respect for private life is a fundamental constitutional right in Hungary, and relevant studies in Hungary[32] cite the decision of Germany's federal Constitutional Court (*Bundesverfassungsgericht,* BVerfG) on so-called online searches *(Online Durchsuchung*[33]*)*. In this case, the BVerfG declared a fundamental right to the integrity and privacy of closed communication networks (IT systems), and in conclusion banned the *Land* authority in charge of constitutional protection from monitoring online communications on such networks using spyware (spy software as a covert instrument), and from searching the contents of personal computers using such spyware. The so-called IT decision adopted in these criminal proceedings deduced the fundamental right to the integrity and privacy of IT systems from general personal rights *(Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)*. The BVerfG deduced this

[32] Sulyok, M., A bizalmi kapcsolattartás bizonyítási védelme a magyar polgári eljárásban – alkotmányjogi szempontok, Eljárásjogi Szemle, 2017(2), pp. 1–30.

[33] BVerfG, 1 BvR 370/07.

protection of rights from Articles 1, 2, and 10 of Germany's Constitution (*Grundgesetz,* GG), and by adopting this interpretation also ensured the protection of privacy for email communication. Sulyok says that: "This fundamental right – as a possible manner of transposing regulations laying the foundation for the privacy and integrity of IT systems the adoption of legislation – may refine the framework system for the protection of fundamental rights (e.g., as regards the rules of exclusion created with respect to this) and law application or constitutional interpretation process of not only Hungary, but also other European countries in relation to information rights and electronic privacy. This German 'right to privacy' is capable of protecting privacy in information society at once as a participation right and a protection right."[34] The German IT decision is in accord with the statements[35] made by the Hungarian Constitutional Court in their fundamental decisions, according to which "modern constitutional practice stipulates general personal rights – as matriarchal rights – through its various aspects (e.g., right to privacy), which can always be referenced if there is no specific fundamental right protecting the given segment. The Constitutional Court's recent practice of interpreting and applying Article VI[36] (following the entry into force of the new Fundamental Law on 25 April 2011) – in addition to confirming their earlier resolutions[37] – opens new ways to protect privacy by stipulating areas of privacy generally protected by the Constitution – such as private and family life (intimacy), home (spacial privacy), communication and reputation (wider privacy) –, and by declaring the 'particularly close' link between the right to dignity and the right to privacy."[38]

4. Execution of telecommunications interception

a) Ordering access providers to extract and surrender specific communications

While the installation of the monitoring sub-system suitable for secret surveillance is the responsibility of electronic communications service providers (Section 92 Paragraph (5) E-Communications Act), the actual secret information gathering (interception) is performed by the NSSS in accordance with the previously defined specifications. This means that during the interception, the entity performing the interception does not order the service provider to extract and hand over the

---

[34] Sulyok, M., A bizalmi kapcsolattartás bizonyítási védelme a magyar polgári eljárásban – alkotmányjogi szempontok, Eljárásjogi Szemle, 2017(2), p. 14.

[35] 8/1990 (IV.23.) Decree of the Hungarian Constitutional Court.

[36] The right to respect for private and family life, home, communication, and reputation, and the fundamental right to the protection of personal data and to access to and dissemination of data of public interest.

[37] 3038/2014 (III.13.) Resolution of the Constitutional Court, reasoning.

[38] 17/2014 (V.30.) Resolution of the Constitutional Court, reasoning; Sulyok, M., A bizalmi kapcsolattartás bizonyítási védelme a magyar polgári eljárásban – alkotmányjogi szempontok, Eljárásjogi Szemle, 2017(2), p. 15.

required data, as the service provider is not involved in the process of interception beyond the installation of the monitoring sub-system and the technical specifications: "Organisations authorised to conduct secret information gathering may only forward data to electronic communication service providers, which are essential for the service providers to meet their obligations related to secret information gathering" (Section 9 Government Decree No. 180/2004). Electronic communications service providers are not entitled to collect, archive or display data generated in the monitoring sub-system in relation to secret information gathering. If the obligations cannot be met without displaying the information, in exceptional cases where the personal involvement of the service providers staff is required it is allowed to display the data (Section 11 Paragraph (1) Government Decree No. 180/2004). Employees of electronic communications service providers may only be involved in secret information gathering activities if they cannot be implemented using technical tools or other solutions of a technical nature (Section 11 Paragraph (2) Government Decree No. 180/2004).

b) Types of accompanying investigative measures

During the use of covert instruments and secret information gathering, any method may comply with legal regulations, which does not result in mass (untargeted) surveillance. In the cases *Zakharov v. Russia*[39] and *Szabó and Vissy v. Hungary*[40] the jurisprudence of the ECtHR summarised their expectations by ruling that surveillance should always be limited to clear period of time. The new CP Act regulates this by using an instrument-based approach to interception: any number of instruments may be used against one person (instrument multiplication), but the surveillance may not last longer than 90 days at any one time, and 360 days altogether. One single authorisation is required for intercepting the communications of a single person, which may be extended based on the data of the procedure, e.g., when the interception has to be extended to other instruments. This can be ordered by the judge in charge of the investigation upon a request from the public prosecutor.[41]

The entitled organisations may use several different methods of secret information gathering at the same time in a complementary manner. This includes in particular: "During a secret search, the bodies entitled to use covert instruments may search in secret – with the exception of public spaces or those open to the public – residential homes, other premises, confined spaces, and – with the exception of means of community transportation – vehicles, and objects used by the person

---

[39] *Roman Zakharov v. Russia*, judgment of 4 December 2015, no. 47143/06.

[40] *Szabó and Vissy v. Hungary*, (n 2).

[41] Interview with a prosecutor who was member of the drafting committee of the new CP Act.

concerned with a judge's authorisation, and may record their findings with technical solutions" (Section 232 Paragraph (2) new CP Act). "During the secret surveillance of a location, the bodies entitled to use covert instruments may – with the exception of public spaces or those open to the public – secretly observe and record with technical solutions the occurrences at residential homes, other premises, confined spaces, and – with the exception of means of community transportation – vehicles. To achieve this, the necessary technical instruments can be installed at the location of use" (Section 232 Paragraph (3) new CP Act). "When secretly accessing messages/consignments, the body entitled to use covert instruments may with a judge's authorisation secretly open letters/parcels sent by post or otherwise, may have access to its contents, and may control and record such" (Section 232 Paragraph (4) new CP Act). "During interception, the body entitled to use covert instruments may with a judge's authorisation secretly access and record the contents of communication transmitted by way of an electronic communication network or device as part of an electronic communication service, or on an information technology system" (Section 232 Paragraph (5) new CP Act).

The police may as part of its secret information gathering activities, without judicial authorisation and in the interest of meeting its law enforcement obligations: "a) use an informant, a person of trust or another person secretly cooperating with the police; b) gather information or control data by disclosing the aim of the proceedings or by using a covert detective revealing his identity; c) issue and use covert documents for the cover and protection of its staff and other cooperating persons, and their affiliation with the police, create cover and maintain organisations; d) keep under surveillance persons suspected of a crime and persons in contact with them, and also spaces, buildings, and other facilities, sections of terrain and roads, vehicles and events, gather information about these, and record observed events with a technical instrument for recording sound, image or other signals or traces; e) set a trap in order to uncover the perpetrator of a crime or to provide evidence in a manner that does not result in injury and is not harmful to health; f) use informants, persons of trust, other persons secretly cooperating with the police and undercover detectives to perform sample purchases, and – with a public prosecutor's authorisation – use undercover detectives for managing controlled delivery, covert purchase, or incorporation into a criminal organisation; g) if there is no other option for preventing or detecting the crime, apprehending the perpetrator, or establishing their identity, substitute the victim in their role – in order to protect the victim's life and health – by using a member of the police force; h) gather information from communication systems and other data storage devices" (Section 64 Paragraph (1) Points a–h) Police Act). As part of operations subject to judicial authorisation, for law enforcement purposes in relation to serious crimes, until investigations are ordered, the police may "a) search private residences in secret, and may record the findings with technical instruments, b) observe and record occurrences at private residences with the help of technical instruments, c) open and control

letters/parcels sent by post and other closed consignments linked to an identifiable person, and record the contents with technical instruments, d) have access to the contents of communication transmitted through an electronic communication service, and record the findings with technical instruments, e) have access to, record, and use data transmitted through or stored on an information technology device or system" (Section 69 Paragraph (1) Points a–e) of Police Act).

As part of secret information gathering activities subject to external authorisation national security services may: "a) request information; b) gather information without revealing their purpose as national security; c) enter into secret contact with a private person; d) create and use information technology systems promoting information gathering; e) use traps without causing injury or damage to health; f) issue and use covert documents for the protection of their staff and other cooperating natural persons, and as a cover of their ties to national security; g) create and maintain cover organisations; h) keep under surveillance persons targeted during their activities, and spaces, buildings, and other facilities, sections of terrain and roads, vehicles and events related to such, and record the occurrences with technical instruments; i)may intercept conversations beyond those under Section 56, and record such with technical instruments; j) gather information from communication systems and other data storage devices" (Section 54 Paragraph (1) Points a–j) NSSA). Subject to external authorisation, the national security services may: "a) search residential homes in secret, and record the findings with technical instruments, b) observe and record occurrences at residential homes with the help of technical instruments, c) open and control letters/parcels sent by post and other closed consignments linked to an identifiable person, and record the contents with technical instruments, d) have access to the contents of communication transmitted through an electronic communication service, and record the findings with technical instruments, and access data transmitted through or stored on an information technology device or system, record the contents of such with technical instruments, and use them" (Section 56 Points a–e) NSSA).

5. Duties of telecommunications service providers to cooperate

Electronic communications service providers have the obligation to preserve and hand over data under the CP Act, the E-Communications Act, the Police Act, and the NSSA. This means that they have an obligation to participate in criminal proceedings for the purposes stipulated in legislation.

a) Definition of electronic communications service provider

Section 188 Point 13 E-Communications Act

Electronic communication service: a service usually provided against a fee, which in part or mostly consists of the transmission of signals through electronic communication networks, and where applicable, the control of such, including data exchange services,

and also public data exchange services, but does not include services providing content using electronic communication networks and services, or exercising editorial supervision over such content, and does not include services related to the information society, and defined in other legal regulations, which do not primarily consist of the transmission of signals through electronic communication networks.

Section 188 Point 14 E-Communications Act

Electronic communication service provider: the operator of an electronic communication network, and the natural or legal person providing an electronic communication service.

b) Data retention regulation and CJEU ruling

Despite the 2014 Court of Justice of the European Union (CJEU) ruling,[42] the Hungarian act allowing data retention is still in force. In April 2014 the Hungarian Civil Liberties Union (HCLU) announced that they would commence lawsuits against Telenor Hungary and Vodafone Hungary in order to force the Hungarian Constitutional Court to repeal the unlawful act. Due to peculiarities of Hungarian law and, specifically, the Jurisdiction of the Constitutional Court, the HCLU cannot directly engage the Constitutional Court to establish that the legislation on the obligation of data protection is against the Fundamental Law of Hungary. Instead, it had to bring a court action against service providers concerning the elimination of data and either (i) request the judge to refer the case of the Constitutional Court for a decision, or (ii) if it eventually lost the lawsuit then commence proceedings directly at the Constitutional Court. During the trial, upon the request of HCLU, the judge referred the Hungarian data retention provisions to the Constitutional Court (see (i) above). However, in 2015 the Constitutional Court rejected to the case for procedural reasons without a decision on the merits. After HCLU lost both at first and second instance the Hungarian courts rejected their case against Telenor Hungary. On 7 April 2016 the Metropolitan Appeal Court confirmed the first instance decision, emphasising that the current legislation is indeed applicable and it would be the legislator's task to propose a new law in order to comply with the Charter and case law of the CJEU. On 7 July 2016 the HCLU submitted their request to the Constitutional Court to repeal the Hungarian data retention provisions (see (ii) above). This case is still pending and there is no information as to when the Constitutional Court will make its decision.[43]

---

[42] Court of Justice of the European Communities Joined Cases C-293/12 and C-594/12, 8 April 2014.

[43] The detailed timeline and story of the case is available in Hungarian here: https://tasz.hu/cikkek/adatmegorzes-sokadszor

c) Implications of the CJEU ruling on the local data retention regulation

The telecom regulator, the National Media and Communications Authority (NMCA), has not made any official statement on the subject. According to non-official information from a party interviewed for this research, their standpoint is that the amendment of the data retention provisions in the E-Communications Act should be commenced by the Ministry of National Development as this ministry is in charge of the E-Communications Act. On 24 June 2014 the local data protection authority (National Data Protection and Information Authority) urged the Ministry of National Development to review the data retention provisions in the E-Communications Act and adopt new provisions which comply with the CJEU's ruling and the Charter. According to non-official information, the Ministry of National Development is working on the review but there is no public result available thus far.[44] Neither the above mentioned Ministry nor other governmental bodies have made official statements on the implications of the CJEU ruling in Hungary.

d) Extension of the cooperation duties to application providers

Telecommunications and internet service providers have an obligation to hand over metadata and provide access to communication (content) data to authorities in charge of national security and law enforcement tasks. As a result of the 2016 modification of the E-Commerce Act application providers are also obliged to preserve metadata for no longer than one year and hand it over to the authorities upon request (E-Commerce Act):

Section 13/B

(1) Application providers providing encrypted communication services shall preserve data generated or managed in relation to the messages and comments transmitted using such application, as stipulated under (2) for a period of one year from the creation of such data.

(2) In the case of a request from a body entitled to perform secret information gathering subject to external authorisation the application provider providing services, which ensure encrypted communication shall hand over a) the type of service; b) the identifying data of the subscriber or user of the service needed to use the service, the time of use of the service, the starting and closing times; c) their IP address and port number used for registration; d) their IP address and port number used for using the service; e) the user identifier.

Application service providers may be sanctioned for breaching these provisions (E-Commerce Act):

Section 16/H

(1) If the Authority establishes a breach of the obligations stipulated under Section 3/B or 13/B based on information from the authority entitled to perform secret information gathering, the application provider – a legal person or an organisation without legal per-

---

[44] NMCA, interview.

sonality – may be fined HUF 100,000 to 10,000,000 due to the breach of cooperation obligations.

(2) The fine levied for the breach of cooperation obligations may be levied multiple times if the breach is repeated.

(3) The fine for the breach of cooperation obligations has to be paid to the bank account of the Authority.

In accordance with the modification "as a result of technical development, internet-based global communication networks and services are increasingly widespread and have become affordable. For this reason there is a realistic risk that general communication habits change, and criminal circles will use these instead of traditional communications service providers. With respect to the fact that mobile applications – one of the elements of the system protecting mobile communications – can be found on the online platforms of application providers for commercial purposes and can be installed from there, thereby preventing the secret services of countries from obtaining the communication or information related to it, and from decrypting such. Stipulating legal obligations for application providers may represent a possible solution to the problem. […] The aim of the modification of the E-Commerce Act was to create the obligations of the service providers for data preservation, data transmission and cooperation. The […] modification of the E-Commerce Act on the one hand creates the opportunity for the service provider's obligation to hand over all data and information essential for the use of secret information gathering instruments and methods, also including information on encryption levels, and on the other the modification stipulates a compulsory agreement for service providers to be concluded with the National Security Special Service on the conditions of secret information gathering."[45]

e) Sanctions against service providers

Service providers and "organisations addressed by data requests" may be fined as part of criminal proceedings, if they do not meet the requirements of the data request by the deadline (default 30 days, in urgent cases 8 days),[46] refuse to meet it without due justification, or breach the rules on disclosing information on data requests (e.g., endangering the success of the criminal proceedings, informing the person named in the data request or others – i.e., exceeding their competence to inform) (Section 265 Paragraph (1) new CP Act). If certain conditions are met, coercive measures – seizure of the requested data, arrest of the person in charge of data requests – may also be used against the service provider (Section 265 Paragraph (1) new CP Act).

---

[45] Reasoning to proposed act T/10307 on the modification of certain acts related to counter-terrorism action, available at https://itcafe.hu/dl/cnt/2016-04/127478/10307.pdf

[46] Telecommunications service providers, interview.

If the access provider does not meet their obligation to make electronic data temporarily or permanently inaccessible, the National Media and Infocommunications Authority may fine the service provider (Section 92/A Paragraph (3) E-Communications Act).

6. Formal prerequisites of interception orders

a) Interception ordered under criminal proceedings

aa) Authorisation of interception orders under "normal" circumstances

Covert instruments may be used under criminal proceedings a) without authorisation, b) subject to a public prosecutor's authorisation, and c) subject to a judge's authorisation (Section 214 Paragraph (4) new CP Act). Covert instruments, which do not require authorisation include persons cooperating in secret, setting traps, and secret surveillance (Section 215 new CP Act). Covert instruments subject to a public prosecutor's authorisation include the surveillance of payment transactions (Sections 216–218 new CP Act), surveillance performed with the consent of the victim (due to usury crimes, harassment, or crimes committed by making threats) (Section 220 new CP Act), covert purchase (Section 221 new CP Act), and using a covert detective (Sections 222–224 new CP Act). Covert instruments subject to a judge's authorisation include the secret surveillance of information technology systems, secret searches, secret surveillance of a location, secret access to messages/consignments, and interception (Section 231 new CP Act).

bb) Authority to authorise the interception

The authorisation to use covert instruments subject to a judge's authorisation is decided by a court based on the proposal of a public prosecutor (Section 236 Paragraph (1) new CP Act).

cc) Formal requirements of the application for interception

The application of the public prosecutor has to contain the reasoning for the interception, and (Section 236 Paragraph (2) new CP Act)

a) the name of the body entitled to use covert instruments, the date of the order for the preparatory proceedings and the investigation, the case's number,

b) available data suitable for the identification of the person named in the application,

c) the planned date (day and hour) of the start and end of the use of covert instruments used against the person concerned subject to a judge's authorisation,

d) the detailed reasoning for the existence of conditions for the use of covert instruments subject to a judge's authorisation, therefore also

da) the categorisation of the crime as per the Criminal Code on which the proceedings are based, the short description of the facts, the data giving rise to the suspicion of the crime or pointing to its possibility,

db) the data proving that the [necessity, proportionality, purpose limitation] conditions stipulated under Section 214 Paragraph (5) are met, and

dc) the aim of the use of covert instruments subject to a judge's authorisation,

e) the name of the covert instruments intended for use,

f) data suitable for the identification of the information technology system in the case of the secret surveillance of IT system; the space, vehicle or object in the case of secret searches; the space or vehicle in the case of the secret surveillance of a location; the place of posting or receipt, or the sender and addressee in the case of secret access to mail/consignments; data suitable for the clear identification of electronic communication service or device, or IT system in the case of interception.

(3) the documents supporting contents of the application shall be attached to it.

b) Interception ordered in law enforcement proceedings of the police

aa) Authorisation of interception under "normal" circumstances

The police may use secret information gathering both without a judge's authorisation (Section 64 Police Act) and with a judge's authorisation (Section 69 Police Act) in the interest of performing their law enforcement tasks. The police may gather information from communications systems and other data storage devices as part of secret information gathering not subject to a judge's authorisation (Section 64 Paragraph (1) Point h) Police Act). The head of the investigative body of the police authorised to perform secret information gathering may with the authorisation of a public prosecutor submit a data request to, e.g., electronic communication service providers (data request procedure) (Section 68 Police Act). However, the access to and the recording of the contents of communications transmitted through an electronic communications service, and the access to and recording of data transmitted in an IT system (e.g., through keyloggers or other spyware) ("interception") is always subject to a judge's authorisation (Section 69 Paragraph (1) Points d–e) Police Act) ("use of special instruments").

bb) Formal requirements

The request for the "use of a special instrument" is submitted by the head of the intelligence organisation of the police to the court *in writing*. The request has to contain (Section 70 Paragraph (2) Police Act)

a) the place of use of the special instrument, the person targeted by the use, and the available data suitable for identification,

b) the name of the special instrument intended for use,

c) the planned start and end (day and hour) of use,

d) the reasoning for the existence of legal conditions for the use.

c) Interception for national security and defence purposes

aa) Authorisation of interception under "normal" circumstances

National security services (Information Office *[Információs Hivatal]*, Office for Constitutional Protection *[Alkotmányvédelmi Hivatal]*, the Military National Security Service *[Katonai Nemzetbiztonsági Szolgálat]*, the National Security Special Service, and the Anti-Terror Information and Criminal Analysis Centre: Section 1 NSSA) may carry out secret information gathering not subject to an external authorisation (Section 54 NSSA) and subject to an external authorisation (Section 56 NSSA). Information gathering from communication systems and other data storage devices (data carrier searches) is a form of secret information gathering, which does not require an authorisation in itself (Section 54 Paragraph (1) Point j) NSSA). However the access to and the recording of the contents of communications transmitted through an electronic communications service, and the access to and recording of data transmitted through and stored on an IT system (e.g., through keyloggers or other spyware) ("interception") is always subject to authorisation (Section 56 Paragraph (1) Points d–e) NSSA).

bb) Authorities to authorise the interception

A proposal for interception may be submitted by the director general of the Information Office, the Office for Constitutional Protection, the Military National Security Service and the National Security Special Service.

In certain cases, the secret information gathering is authorised by the judge appointed by the president of the Municipal Tribunal of Budapest for this task (Section 58 Paragraph (1) NSSA), in other cases, so e.g., as regards data requests from data management systems (stipulating the goal of the data request) (Section 40 Paragraph (1) NSSA) the secret information gathering is authorised by the Minister for Justice (Section 58 Paragraph (2) NSSA). The aim of the secret information gathering and the gravity of the crime determine which body issues the authorisation. (The decision in the case *Szabó and Vissy v. Hungary* declared specifically that these secret data interception measures authorised by a minister – and not a judge – were in violation of the Charter and its provision on the respect for private life. The cited Section of the NSSA in effect since July 2016 which makes data requests possible from any data management systems for national security purposes does not put an end to the severe restriction of fundamental rights, and what is more, it extends the areas of secret information gathering of the national security services.[47]

---

[47] HCLU, A Társaság a Szabadságjogokért álláspontja a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló törvény tervezetéről, 2016, available at https://tasz.hu/files/tasz/imce/a_tasz_allaspontja_a_terrorizmus_elleni_fellepessel_osszefuggo_egyes_torvenyek_modositasarol_szolo_torveny_tervezeterol.pdf

cc) Formal requirements

The request for interception has to contain (Section 57 Paragraph (2) NSSA):

a) the place of secret information gathering, the name or group name of the persons concerned, and if possible the available data suitable for identification;

b) the description of the secret information gathering and the reasoning for its necessity;

c) the start and end (day and hour) of the activities;

d) in the case of the application for ("exceptional") authorisation stipulated under Section 59, the reasoning why it was essential for the successful operation of the national security service.

d) The applicant's case presented to the competent authority in writing

For the applications, the head of the entitled organisation stipulated in legislation has to submit the (above described) documents requesting the authorisation and those supporting and justifying the authorisation *in writing* (simple, written application).

7. Substantive prerequisites of interception orders

a) Degree of suspicion

If the secret information gathering is ordered *as part of an investigation*, the level of suspicion required for ordering the investigation is needed, i.e., non-qualified suspicion. Before the investigation is ordered, even less than that, i.e., an abstract danger is enough for the secret information gathering. The only distinguishing factor is that no explorative, i.e., non-targeted, surveillance can be ordered during an investigation. This ban is not stipulated in the CP Act (neither the old, nor the new), but rather in the Act on Freedom of Information (Info Act). In the Info Act, rules on data management stipulate that data gathering with a stockpile approach is not possible (the necessity criterion of data management: Section 4 Paragraphs (1) and (2) Info Act). The above-mentioned provisions of the Info Act also stipulate that data management – and within that data gathering – may only be performed in a pre-defined, and appropriately targeted manner, has to be suitable for achieving the goal, and is proportionate, i.e., it meets the requirements of data minimisation. These basic principles are applicable in all phases of data management independent of the authority or body managing the data and in what proceedings they are managed,[48] i.e., also in the phase preceding the investigation and during such, or in the criminal proceedings.

---

[48] Vissy, B., The right to informational self-determination, Paper presented 28 November 2016, at Department of Constitutional Rights, Faculty of Law, ELTE University, Budapest.

One of the most significant reforms of the new CP Act is the stipulation of secret intelligence activities for law enforcement purposes in fundamental legislation on criminal proceedings. According to the new CP, the information gathering may have three phases: (1) preparatory procedure (criminal detection), (2) investigation, and (3) examination (assessment of the data and information gathered). Accordingly, the degree of suspicion demanded by the different phases will also be different: in the preparatory procedure "suspicion preceding simple suspicion" is required, during investigation "simple suspicion," and during examination "justified suspicion." The new act on criminal proceedings thereby creates the opportunity for the investigative authority to keep a person under surveillance for any length of time even without authorisation, as part of the "preparatory procedure" preceding the criminal proceedings. The aim of the "preparatory procedure" (Section 340 Paragraph (1) new CP Act) is defined as identifying whether there is a suspicion of a crime. However, the literal interpretation of the legislation either renders law enforcement completely powerless, or quite the opposite, it may start a process of total action, where it sees suspicion everywhere and in everybody.[49] The legislation declares that "covert instruments subject to a judge's authorisation may be used in a preparatory procedure in the interest of establishing the suspicion of a crime and against a person, who a) may potentially be the perpetrator of the crime […]" (Section 343 Paragraph (1) Sentence I new CP Act). According to interpretations of the law, a lack of suspicion renders the requirements of necessity and proportionality both meaningless; as Finszter and Korinek write "a lack of suspicion leaves law enforcement authorities, and in the end also jurisdiction defenceless against the arbitrary exertion of power, makes it impossible to control that in the rule of law, law enforcement may only be legitimised by the requirements of criminal law."[50]

Under the Police Act, as part of secret information gathering for policing purposes (i.e., in the phase of intelligence measures preceding the "preparatory procedure") the police may in the interest of the detection and interruption of crimes, identifying and apprehending the perpetrator, obtaining evidence, and the recovery of assets resulting from the crime, use covert instruments in accordance with the CP Act (Section 63 Paragraph (4) Police Act). This type of secret information gathering is linked to a fourth, and even more abstract concept of suspicion than preceding the "preparatory procedure" above. Such an extension of the concept of suspicion does not comply with the requirements for the clarity, transparency, and predictability of norms.[51]

---

[49] Finszter G., Korinek L., Az eltűnt gyanú nyomában, Belügyi Szemle 2018(3), pp. 104–122.

[50] Finszter G., Korinek L., Az eltűnt gyanú nyomában, Belügyi Szemle 2018(3), p. 121.

[51] *Ibid*.

b) Authorisation, scope of crimes, period of applicability of secret information gathering

As secret information gathering (interception) is regulated both by legislation on the police and the national security services, the provisions of both Acts will be discussed.

The new CP Act regulates secret information gathering in the chapter on covert instruments (Part 6: Sections 214–255 new CP Act). Covert instruments may be used in criminal proceedings subject to a judge's authorisation or a public prosecutor's authorisation, or without an authorisation – as long as the conditions of necessity and proportionality are met. Interception – which includes the surveillance and recording of electronic communications in the systems of electronic communications service providers – is subject to a judge's authorisation (Section 232 Paragraph (5) new CP Act). The judge decides on the basis of the public prosecutor's proposal (Section 236 Paragraph (1) new CP Act). The content requirements for the proposal are stipulated in the new CP Act (Section 236 Paragraph (2)).

If the authorisation results in a delay, which would significantly endanger the desired goal, the public prosecutor's office may order a "secret search," or may up to the decision of the court, but for no longer than 120 hours, order the use of covert instruments (Section 238 Paragraph (1) new CP Act). If that is the case, the public prosecutor's office still applies to the court within 72 hours of the order for a post-authorisation, on which the court must decide within 120 hours. If the authorisation is not granted, the information acquired through the use of covert instruments may not be submitted as evidence, and the data has to be deleted immediately (Section 238 Paragraph (5) new CP Act).

The court may authorise the use of covert instruments for a maximum of 90 days, which may be extended by a further 90 in each case, and may not be longer than 360 (Section 239 new CP Act).

Covert instruments subject to a judge's authorisation may be used in relation to intentional crimes punishable by imprisonment of up to five years or more (Section 234 Paragraph (1) new CP Act). It may also be used in relation to the following intentional crimes punishable by imprisonment of up to three years (exhaustive list): a) crimes committed on a commercial scale or in a criminal association, b) criminal offences with drug precursors, forgery of health products, c) sexual abuse, pandering, procuring for prostitution, living on earnings from prostitution, exploitation of child prostitution, child pornography, d) environmental offences, damaging the natural environment, poaching, organisation of illegal animal fights, violation of waste management regulations, e) crimes against the judicial system with the exception of breach of seal, f) with the exception of failing to report a corruption crime, crimes of corruption, g) criminal offences related to elections, referendums, and European citizen's initiatives, unlawful employment of a citizen of a

third country, organisation of illegal gambling, h) insider dealing and illegal market manipulation (Section 234 Paragraph (2) Points a–h) new CP Act).

The new CP Act stipulates an opportunity for "data gathering" for the purpose of establishing the suspicion of a crime, or the existence of evidence for a crime in a so-called preliminary procedure (Section 267 Paragraph (1) new CP Act). The public prosecutor's office, the investigative authority, the internal crime prevention and crime detection body of the police, the anti-terror unit of the police, and after the indictment the public prosecutor's office are entitled to do this. During data gathering electronic communications service providers may not be approached to hand over data, but data can be gathered from public databases (Section 267 Paragraph (3) Point b) new CP Act).

The police may perform secret information gathering in order to prevent or detect crimes, and to obtain evidence (Section 63 Paragraph (1) Police Act). The secret information gathering of the police may or may not be subject to a judge's authorisation. The police may gather information from communications systems and other data storage devices as part of secret information gathering not subject to a judge's authorisation (Section 63 Paragraph (1) Point h) Police Act). The head of the investigative body of the police authorised to perform secret information gathering – with a public prosecutor's approval – may request the handover of data in relation to the case in the interest of the detection of intentional crimes punishable by imprisonment of up to two years or more and the recovery of assets resulting from the crime, e.g., from the electronic communications service provider, and healthcare bodies and other organisations managing related data; and also data classified as bank secrets, payment secrets, securities secrets, insurance secrets, and business secrets from the organisation managing such data. The investigative organ may stipulate a deadline for meeting the data request. The handover of data is free of charge and may not be denied. Information thus obtained may only be used for the stipulated purpose (Section 68 Paragraph (1) Police Act). The police may request the above-mentioned service providers to hand over data in relation to their crime prevention and detection tasks, and the anti-terror unit of the police in relation to detecting intentional crimes punishable by imprisonment of up to two years or more, with the approval of a public prosecutor may request the handover of data from the above-mentioned service provider (Section 68 Paragraph (1a) Police Act).

As *an urgent measure*, if a delay results in danger, and the case is related to drug trafficking, terrorism, illegal arms trafficking, money laundering or organised crime, the prior approval of the public prosecutor is not required for the data request, which has to be met immediately. At the same time as the data request, measures have to be taken to obtain the public prosecutor's authorisation. If the public prosecutor refuses to issue an approval, the police destroys the data obtained by the action immediately (Section 68 Paragraph (2) Police Act). As part of their secret information gathering activities subject to a judge's authorisation, the police may for law enforcement purposes and in the case of serious crimes – which are

listed under Section 69 Paragraph (3) of the Act –, e.g., have access to the contents of communications transmitted by way of an electronic communications service, may record such contents with technical solutions, may have access to, record and use data stored on or transmitted by way of computer system (Section 69 Paragraph (1) Point d–e) Police Act).

Data related to persons obviously not targeted by the proceedings have to be destroyed immediately, and may not be managed or used further (Section 69 Paragraph (2) Police Act).

The judge authorises the use of "special instruments" for secret information gathering for 90 days in each case, which upon request may be extended by another 90 days (Section 71 Paragraph (3) Police Act). If the authorisation would result in a delay, which would be contrary to the interest of a successful law enforcement action, the head of the investigative authority may order a secret search, and for a duration of 72 hours the use of special instruments ("emergency order") (Section 72 Paragraph (1) Police Act). In the case of an emergency order, the request for authorisation has to be submitted at the same time. If the request is rejected, an emergency order may not be issued for the same purpose with the same reasoning and based on the same facts (Section 72 Paragraph (2) Police Act).

In addition to the investigative authority (prosecutor, police – as regulated by the CP Act) and the police (as regulated by the Police Act), national security services may also conduct secret information gathering in accordance with the requirements of necessity, i.e., if the data needed for performing their tasks stipulated in legislation cannot be obtained in any other way (Section 53 NSSA). Secret information gathering activities may be performed subject to an external authorisation or without it. Without an external authorisation they may, e.g., create and use information technology systems promoting information gathering (Section 54 Paragraph (1) Point d) NSSA); and may gather information from communication systems and other data storage devices (Section 54 Paragraph (1) Point j) NSSA). In order to promote the latter activity, communications service providers have to ensure the installation of a monitoring sub-system needed for secret information gathering. The monitoring sub-system is installed in accordance with the cooperation agreement concluded with national security services, at the service provider's own technical facilities, and at his own cost.[52] Subject to an external authorisation, national security services may among other things: have access to the contents of communications transmitted through an electronic communications service, may record the accessed contents with technical solutions, and may have access to, record and use by way of technical instruments data stored on or transmitted through information technology devices and systems (Section 56 Paragraph Points d) and e) NSSA). Secret information gathering subject to an external authorisation is authorised by

[52] Communications service providers, interview.

the court appointed for the purpose or the Minister of Justice based on the application of the director general of the given national security body (Section 58 Paragraph (1) NSSA). Secret information gathering activities subject to an external authorisation include those which severely restrict citizens' rights, such as the interception of citizens' electronic communications. Secret surveillance in relation to the protection of state sovereignty or constitutional protection lies within the competence of the Minister of Justice, while authorisation for secret surveillance for law enforcement purposes requires a judge's authorisation in relation to crimes against the state and military crimes. If an authorisation from the Minister of Justice or a judge is needed for accessing the contents of communications transmitted through an electronic communications network, the services needed by organisations entitled to conduct secret information gathering are rendered by the National Security Special Service with conditions stipulated in separate legislation (Section 8 Paragraph (1) Government Decree No. 180/2004). Surveillance not subject to an external authorisation includes measures which restrict citizen's rights to a lesser extent, e.g., route monitoring, installing a CCTV system, and surveillance for the protection of individuals or facilities. There are requirements in place for the contents of requests for authorisation (Section 57 Paragraph (2) NSSA). Authorisations may be issued for 90 days, which may be extended by a further 90 days based on a separate application (Section 58 Paragraph (4) NSSA). If the external authorisation would result in a delay, which would be contrary to the interests of national security in the given case, the directors general of the national security services may authorise secret information gathering (Section 59 Paragraph (1) NSSA). Such "emergency authorisation" may only be ordered once in a single case.

c) Possible subjects of an interception order

The person targeted by the surveillance with covert instruments is precisely identified by the public prosecutor in their application for the use of covert instruments (Section 236 Paragraph (2) new CP Act). The use of covert instruments may also be extended subject to a judge's authorisation, e.g., when the observation of another electronic communications service or another information technology system becomes necessary (Section 241 Paragraph (1) new CP Act).

d) Targeting particular communications content

Surveillance targeting communications content (e.g., lead by automated trigger words) is not possible under legal regulations, as its purpose is not limited, it would be considered data stockpiling. So-called "reliability tests" conducted internally at the public prosecutor's office, the investigative authority, the police and the national security services represent an exception from this, where such keyword-based data stockpiling is admissible (Sections 7–7/G Police Act, Government Decree

No. 293/2010 (XII. 22.), Section 29 Paragraph (6) Public Prosecution Act, Chapter VII of Directive No. 3/2012 (I.6.) Prosecutor General's Office.[53]

e) Consent by a communications participant to the measure

The new Criminal Proceedings Act introduces the legal institution of "interception used with consent," and stipulates that "The body entitled to use covert instruments may use surveillance with the authorisation of the public prosecutor's office and the written consent of the victim a) usury crimes, harassment, domestic violence or b) crimes committed by making threats." (Section 220 Paragraph (1) new CP Act). As harassment and domestic violence are often perpetrated using electronic devices, this legal institution will probably be used frequently.[54] In addition, the Act contains a special condition for access to communications through electronic communications services: "During surveillance with a consent the body entitled to use covert instruments may have access to the communication of the person defined under Paragraphs (1) and (2) transmitted through an electronic communication service, on an electronic communication network or device, or on an information technology system, may record its findings with technical instruments, and may have access to the personal data of the persons involved in the communication" (Section 220 Paragraph (4) new CP Act). The use of surveillance with consent may be authorised for up to 45 days.

8. Validity of interception order

In the case of surveillance for specific law enforcement purposes authorised by a judge – secret information gathering, secret data interception – the period of surveillance has to be precisely specified (e.g., "the period of the target person's stay in Hungary, expected to last 5 calendar days," or for the duration of the event under surveillance, the duration of the foreign delegation's visit, etc.). There is no upper limit to the duration of surveillance for specific law enforcement purposes authorised by a judge.

Surveillance and data handover can be ordered any number of times. In relation to "reliability tests" there is a limit to frequency, as this represents explorative data gathering with the organisation of the investigative authority and the public prosecutor's office. During these tests, the given person is tested randomly, but it is always a concrete fact that is tested.

---

[53] For summary see Bejczi, A., Célpontban a megbízhatósági vizsgálat, Belügyi Szemle 60(6), 2012, pp. 24–65.

[54] National Investigation Bureau, interview.

9. Duties to record, report, and destroy

A final report has to be drawn up, not for the authorising entity, but for the authority who will rely on the obtained information as evidence in the proceedings. It is this final report that is later used as evidence. This is stipulated in the Criminal Proceedings Act: "the body performing the secret surveillance draws up a final report about their findings" (Section 243 Paragraph (1) new CP Act).

10. Notification duties and remedies

The authorising entity does not inform the person concerned by the secret information gathering about the fact of surveillance, not even when the surveillance is over (Section 58 Paragraph (6) NSSA), but only if and when the surveillance is followed by a criminal procedure. Similarly, if the police or other investigative bodies conduct secret information gathering, the person concerned has to be informed when the secret information gathering is over and followed by a criminal procedure. However, in the case of a preparatory procedure, which precedes the criminal proceedings, the targeted person does not know that he is under surveillance, therefore he has no opportunity to lodge a complaint or claim damages. Remedy is only possible, when the information gathering is disclosed, i.e., when it is used as evidence in court. This is when the order's lawfulness, legality, usability, and the legality of the acquisition of data can be contested. It is important that the legal representative may access the classified data which was disclosed after the surveillance ended. A closed hearing has to be held due to the classified data, but the legal representative may access the given data and ask for it to be excluded from the evidence, e.g., due to the fact that the conditions for secret surveillance were not met, or that it was not used in relation to a crime specified in legislation, or that the final report was not drawn up by the deadline. If, however, the preparatory procedure was not successful, i.e., the information gathered during the preliminary procedure did not lead to the initiation of criminal proceedings, the targeted person will not know at the end of the preliminary procedure that he was under surveillance and that data was gathered about him.

11. Confidentiality requirements

a) Confidentiality obligation for internet providers

Electronic communications service providers have a confidentiality obligation as regards their legally required contribution to secret information gathering. This is regulated by two legal regulations: Government Decree No. 180/2004 stipulating the cooperation of electronic communications service providers in secret information gathering, and the Classified Data Act. "Only persons may participate in activities related to secret information gathering, and the installation, operation,

system supervision, repair and maintenance of monitoring sub-systems and devices, who passed the national security screening stipulated in the National Security Services Act, and has a contract issued by an executive of the electronic communication service provider with the consent of the National Security Special Service" (Section 13 Government Decree No. 180/2004). The security requirements are regulated by the Classified Data Act: "Electronic security measures have to be taken to ensure the confidentiality, integrity, and availability of the electronic system and the classified data managed on it" (Section 10 Paragraph (7) Classified Data Act). All cooperating persons with access to the data receive a "personal security certificate," which is issued by the National Security Supervisory Authority (Section 17 Paragraph (2) Classified Data Act).

– *Sanctions for breach of the confidentiality obligation*

The members of electronic communications service providers participating in secret information gathering shall be punishable for the crime of "abuse of classified data" if they breach their obligation of confidentiality: "Persons entitled to use classified data under legal regulations, who abuse classified data, where such data is of limited publicity, confidential, secret or top secret […], shall be punishable with imprisonment of two to eight years. Preparations for an offence and negligent behaviour are also punishable" (Section 265 Paragraph (3) Criminal Code).

b) Maintaining the integrity and reliability of the material obtained

The "electronic data" obtained from the system of an electronic communications service may be forwarded to the investigative authority in different ways: a) in the automatic data request system, b) if the service provider performed a manual query and breakdown, on a data carrier (formerly CD or DVD, today mostly USB flash drive), c) through the monitoring sub-system developed for secret information gathering – in which case the data has to be de-classified first (Sections 256–260 new CP Act). The data obtained in the automatic data request system is sent to the investigative authority with a time stamp and digital signature. The data carriers handed over by service providers and data carriers containing data obtained during secret information gathering are first seized by the investigative authority, then an authenticated copy of them is made, and sent to the IT expert. It is the authenticated copy with the opinion of the expert attached that will have probative value in the criminal proceedings. The court may in accordance with the principle of directness summon persons participating in the data interception – a member of the investigative authority present at the house search or seizure, or the member of the NSSS participating in the secret information gathering – to a hearing in the process, to answer the questions of the court verbally, as a witness. The questions may refer to the acquisition of data, and the conditions of data acquisition. The testimony in court represents a part of the evidence procedure, but does not add to the list of evidence (unless new evidence emerges in relation to the testimony).

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

a) General overview

Electronic communications service providers have the obligation to preserve and hand over data under the E-Communications Act, the Police Act, and the NSSA. This means they have a cooperation duty for purposes stipulated in legislation.

Electronic communications network operators and providers of electronic communications service shall be required – for the purpose of compliance with any request made by the investigating authority, the public prosecutor, the court or the national security service pursuant to the authorisation conferred in specific other legislation, with a view to discharging their respective duties – to retain certain data generated or processed by the service provider in connection with the provision of electronic communications services relating to the subscribers or users of such electronic communications services. This obligation is basically the implementation of the DRD. Even though the CJEU declared latter invalid, the Hungarian data retention obligations are still in force and binding on electronic communications service providers.

b) Local regulation basis for retention of data

Article 159/A. (1) was inserted to the E-Communications Act by Act 174 of 2007 with effect from 15 March 2008 in order to comply with the DRD. Table 1 below contains the type of data collected, including the regulatory sections and the timeframe of how long the given type of data is stored according to the law.

Table 1

Hungarian E-Communications Act, Section 159/A. Paragraph (1)	**Retention time**
a) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, *the personal data specified in the subscriber agreement;*	For a period of one (1) year following termination of the subscriber agreement
b) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, *the telephone number allocated to the terminal equipment of the user or subscriber or to the subscriber access point, or the user ID or any technical identifier fixed in the subscriber contract or otherwise assigned to the subscriber or user by the provider of electronic communications services;*	

c) in connection with fixed network telephony services, fixed internet access services, or the combination of these, *the address where the terminal equipment of the user or subscriber or the subscriber access point is installed, and the type of equipment;*	
d) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, *the telephone numbers of the users and subscribers participating in the communication, their technical means of identification, user IDs, type of electronic communication services involved, and the data necessary to identify the date, time, and duration of a communication;*	For a period of a half (0.5) year from when they were generated
e) in connection with fixed network telephony and mobile telephony services, or the combination of these, *in cases involving call forwarding or call transfer, the subscriber or user number or numbers to which the call is routed;*	
f) in connection with mobile telephony services, concerning *the equipment used at the time of communication, the International Mobile Equipment Identity (IMEI) of the calling and the called party, and the International Mobile Subscriber Identity (IMSI) of the calling and the called party;*	
g) in connection with mobile telephony services, *the location label (cell ID) and network identifier at the start of the communication, and the data identifying the geographic location of cells by reference to their location labels (cell ID) during the period when the service was provided;*	
h) in connection with internet mail services and internet telephony services, or the combination of these, *the data referred to in Paragraph d) of the intended recipient(s) of the communication;*	
i) in connection with internet access, internet mail services, internet telephony services, or the combination of these, *type of the electronic communication service, the date and time of the log-in* and *log-off by the subscriber or, together with the IP address allocated to the communication, and the user ID of the subscriber or registered user, including the calling number;*	
j) in connection with internet access, internet mail services and internet telephony services, or the combination of these, *the data necessary to trace any changes made in the unique identifiers of* subscribers *and users by the provider of electronic communications services (IP address, port number);*	
k) in the case of pre-paid anonymous mobile telephony services, *the date and time of the initial activation of the service and the location label (cell ID) from which the service was activated.*	

Hungarian E-Communications Act, Section 159/A. Paragraph (2)	Retention time
Data listed in *Paragraph* (1) above but in relation to unsuccessful call attempts.	For a period of half (0.5) *year* from when they were generated

c) Assigning dynamic IP addresses

Requesting a list of dynamic IP addresses is possible either by calling on the service provider, or in the automatic data request system. A prerequisite of this is that it has to be determined very precisely for what period of time the entitled body would like a breakdown of all users of the same IP address. It is possible that a single IP address may be used by 30 different users within two days, and it is a lengthy process – including identification, witness research – to filter out the persons relevant for the criminal proceedings. Whether a dynamic IP address can be obtained through the automatic system depends on the mobile and land-line phone coverage of the given region of the country. If a single IP address can be assigned to several users within a short time, entitled bodies usually submit a request to the service provider, who creates the breakdown manually. If the request of the investigative authority references an "above-average" number of users or an "above-average" period, the service provider must also meet such a request, and may not override the goal of the authority. It is sufficient to name only the purpose of the request (in relation to what crime, and in what case the requested data is needed); the service provider does not override the authorities' request, and does not arbitrarily limit the scope of the data.[55] The user data requested by the investigative authority may be used not only for evidence, but also to determine the orientation of the investigation.[56]

d) Refusal to meet data requests

It is not typical in practice that a service provider refuses to meet a data request for law enforcement, defence, or national security purposes. This has formal and content-related requirements (references to legislation, purpose limitation), which the originator of the request complies with. On one occasion Magyar Telekom refused to meet a data request of the police, because it was only signed by the administrator of the case and not his supervisor. As soon as the signature was obtained, the data was handed over. This data request was made many years ago, and the investigative authority submitted the request in writing – the currently effective automatic data request system was not yet in operation. As technologies evolve,

[55] Telecommunications service providers, interviews.

[56] Investigative authority, interview.

paper-based administration is becoming rarer, and at the same time the investigative authority also requests data, whose scope is not regulated precisely by the E-Communications Act. An example of this is that earlier client contracts were only concluded on paper, but today a user contract may also be concluded electronically (through the webshop). Electronically concluded client contracts are not signed by the clients, therefore copies of them are not admissible as evidence, only the IP addresses which are used by the client at the time the contract is concluded. At this point, an understanding had to be reached with the investigative authority: is it the IP address used when entering the webshop, or the dynamic IP assigned during the time spent browsing the webshop that is needed as evidence. In questions like this and similar ones there is a continuous dialogue with the investigative authority.[57]

2. Identification of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

a) Device ID (IMEI)

Data requests for IMEI numbers are met by service providers in accordance with Section 159/A Paragraphs (1) and (2) of the E-Communications Act.

b) Card number (number on the back of SIM cards)

Card numbers may be handed out upon request, service providers meet data requests in accordance with Section 159/A. Paragraph (1) and (2). In relation to missing/wanted persons' data, this may be requested from service providers, which proves whether the given person connected to any telecommunications network in the period. One question can be, e.g., whether a SIM card of a Hungarian service provider was inserted into a stolen phone – service providers are in practice capable of specifying this.[58]

c) IMSI number

With the help of the IMSI number, the activities of a given user on the network may be identified. This is classified data, which service providers do not hand over even upon request, and there is no such authorisation in legislation, not even as classified data as part of secret data gathering.[59]

---

[57] Magyar Telekom, interview.

[58] Vodafone, interview.

[59] Telecommunications service providers, interview.

D. Access to (Temporarily) Stored Communications Data

1. Online searches with the help of remote forensic software

a) Online search in the criminal procedure

The old CP Act (Act XIX of 1998) stipulated that house searches were searches of houses, flats, other premises, confined spaces belonging to these, or vehicles, and of the information technology systems located there, or data carriers containing data stored in such systems in the interest of the success of the procedure (Section 149 old CP Act). Before the old CP Act entered into force in 1998, the list did not contain the provisions of electronic data, therefore there was a debate whether the search of a computer system or a data carrier qualified as a house search.[60]

The decision of the German federal Constitutional Court (2009)[61] declared online searches unconstitutional and defined the right to the confidentiality and integrity of information technology systems as a new fundamental right. It established that the same guarantees have to be ensured for online searches as for secret surveillance, which was not the practice at the time. In Hungary neither the old, nor the new CP Act stipulate the option of online searches separately, but they provide opportunities for that, as secret surveillance subject to a judge's authorisation.[62] This is used in cases, when the analysis of the data is not possible later, nor it is certain that the data will be available unchanged, e.g., in the case of data stored in cloud services.[63]

The new CP Act refers to this coercive measure as "search" *(kutatás)*, which is better suited to its meaning, as it may be applied not only to houses, but also vehicles and information technology systems (Section 302 new CP Act). The scope of the search is extended compared to the old act, as it can also be used, if it leads to the finding of an asset that can or has to be confiscated or the search of an information technology system or data carrier. Data stored on such devices can be considered evidence.

b) Online search through intelligence (interception)

As regards the secret information gathering activities performed by the national security services, there was a recommendation from the data privacy commissioner in 2009 in relation to the problems associated with the use of the spyware FinFisher

---

[60] Laczi, B., A szamitogep es a buntetojog. Magyar Jog 2001(3), pp. 137–152.

[61] BVerfG, 1 BvR 370/07

[62] National Investigation Bureau, interview.

[63] Dornfeld, L., A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések, Belügyi Szemle, 2018(2), pp. 115–135.

used by the National Security Special Service.[64] The data privacy commissioner declared that the group of targeted persons was defined in the then effective Act inaccurately (with a reference to the group of persons), and the Act contained no provision on the deletion of data that was not needed. The delineation between a minister's and a judge's authorisation was also not clear. So far, amendments of the NSSA have not put an end to the divided authorisation system (also under current legislation, either a minister or a judge authorises surveillance), but have made the regulation somewhat more precise. However, the data privacy commissioner highlighted that under the then effective regulation external authorisation only had to be obtained for the interception (secret information gathering) of "messages transmitted on a telephone line in public use or by way of a telecommunication service replacing such," and it was not obvious what rules should apply to accessing and searching computers remotely on a network, or whether an external authorisation was needed at all in such situations. The regulation changed as of 1 January 2011, and now it is a requirement that national security services may only have access to and use "data transmitted through an information technology device or system or stored there" (Section 56 Point e) NSSA).

2. Search and seizure of stored communications data

a) Authorisation of the search of data stored at the service provider

The legal options for access to electronic data stored at the service provider are the same as under general procedural regulations. This means that whatever can be performed only subject to a judge's or public prosecutor's authorisation according to the CP Act, can only be searched with the same authorisation, e.g., emails not yet opened by the addressee can only be accessed with a judge's authorisation by the authorities, and the seizure can also only be ordered by a judge. The communication of a lawyer can only be searched by a public prosecutor (including electronic communications), as only a public prosecutor may investigate crimes committed by lawyers.

b) Seizure of electronic data

There are heated debates among legal experts as what exactly has to be seized during proceedings: the whole information technology system, the data carrier, or only the data.[65] The concept of "seizability" of data was entered into the text of the CP Act by Act CLXXXVI of 2013 on 1 January 2014. Before that, it was common

---

[64] https://atlatszo.hu/2014/09/13/jori-andras-az-internetes-hazkutatasokrol-a-finfisher-ugy-apropojan/

[65] Dornfeld, L., A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések, Belügyi Szemle, 2018(2), pp. 115–135.

practice to seize the whole computer, later, however, only the hard disk drive was seized, and after the CP Act was modified, only the data itself. This contradicts the fact that the data carrier itself is to be confiscated, as it is an instrument of the crime, while others argue that not all information important for evidence may be obtained from the data carrier (e.g., HDD) itself.[66] The seizure of the data may therefore be relevant, if the information technology system is not an instrument of the crime. In such a case, the seizure of the system for a longer period would be excessively detrimental. At the same time, the law does not use such a distinction, it is therefore left to practice to work it out.[67] One of the ways to implement this in practice is if the scope of data to be copied is established during an on-site examination, or an authenticated copy is made of the whole system using a hash key.[68] The former method can be used efficiently on smaller amounts of data, but it may be a problem in the evidence procedure that the result can no longer be reproduced from the original system. The seizure of the data carrier in itself may be problematic, because if the hard disk drive is removed from its original environment, the majority of applications can no longer be run, the version number, etc. cannot be established.[69] It may also happen that certain data is not stored directly on the data carrier, but in a cloud, which is no longer accessible if the data carrier is seized. With respect to the above, literature and the interviewees agree that it is the seizure of the whole system that best serves the interest of the investigation, which may, however, seriously prejudice rights due to the lengthy procedure (the operation of the company affected by the seizure is severely obstructed). On the other hand, a full seizure may infringe the fundamental rights of persons not directly targeted by the proceedings.

The Police Act stipulates that the data can be managed for law enforcement purposes, which are necessary for averting a danger, or the prevention, detection, and evidencing of a specific crime (Section 90 Police Act). A 2009 statement of the data privacy commissioner declared that access to data not necessary for the proceedings should be limited to a reasonable period.[70] According to this recommendation, only the administrator and the superiors of the case, and the IT expert should have access to personal data during the investigation. They work in an investigation environment, where unauthorised persons are excluded. In accordance with the practice of the National Investigation Bureau, an authenticated copy is

---

[66] Vadász, V., A szamitogep demisztifikalasa. Ugyeszek Lapja 2010(2), pp. 13–21.

[67] Dornfeld, L., A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések, Belügyi Szemle, 2018(2), pp. 115–135.

[68] Sorbán, K., Digitális bizonyíték a büntetőeljárásban, Belügyi Szemle 2016(11), p. 81.

[69] Vadász, V., A szamitogep demisztifikalasa. Ugyeszek Lapja 2010(2), pp. 13–21.

[70] Data Privacy Commissioner, A nemzetbiztonsági szolgálatok külső engedélyhez kötött titkos információgyűjtéséről szóló adatvédelmi biztosi ajánlás, Ügyszám:1813/T/2008-4, 2009, available at http://abi.atlatszo.hu/index.php?menu=aktualis/ajanlasok&dok=1813_T_2008-4

made of the whole seized system, which is then examined; this also reduces the number of persons with access.[71] The new CP Act does not separately stipulate the system and the data carrier, and instead stipulates the seizure of electronic data (Section 308 Paragraph (3) new CP Act). This also solves the issue of the seizability of cryptocurrencies, and in addition also precisely specifies the seizability of electronic data suitable for payment (Section 315 Paragraph (2) new CP Act).

c) Seizure of emails

It is also a new regulation that messages transmitted through an electronic communications service (emails) not yet forwarded to the addressee or received in the mailbox but not yet opened by the addressee are seizable before the indictment only at the order of a public prosecutor, and after the indictment only at the order of a judge (Section 309 Paragraph (3) new CP Act). In practice, not yet opened emails (not yet clicked on) can only be accessed by the investigative authority subject to the above authorisations.[72]

d) Practice related to the access to emails

Whether the email has been opened or not by the person targeted by the proceedings can be established by the investigative authority, in several ways:

1. If during a house search on site it can be seen that the computer is turned on and the person concerned is at the moment using their email service, it will be assumed that they have become aware of the content of the emails.
2. If the person is not using an email client (e.g., Outlook), and accesses their emails on an online surface without downloading them, the authority cannot automatically access the mailbox of the user. In such cases the data – the content of the email communication – has to be obtained from the user with his consent or from the service provider. Emails not yet opened and marked as "unread" have to be considered as "not delivered," which the investigative authority may only access with the consent of the user, or if this is not possible (i.e., "the environment is not supportive"), the data has to be seized. This is important for the evidence procedure. This is why screenshots are taken on site during house searches; the photos prove what condition the computer was in, when it was found.
3. If the user uses an email client, and their emails are downloaded to the computer, the police saves the data from the computer. If the emails are stored on a company server, and if the environment is not "adverse" – i.e., the system operators or the user give their consent –, the police access the emails, and save an export. From the saved data it is obvious which emails were opened, and which were not.

---

71 National Investigation Bureau, interviews.

72 National Investigation Bureau, interviews.

It is a further practical question, how "different kinds of information stored on a mobile phone" are mixed, and if the user only gives their consent to the investigative authority to access, e.g., the images, how can the remaining relevant information be accessed? For example, if the chat client was open, but the owner of the mobile device did not consent to accessing it, the investigative authority cannot access it, unless as part of a separate seizure, subject to a public prosecutor's authorisation. Further, if the investigative authority is only granted authorisation to access (seize) the messages appearing on the screen, and not the remaining elements of the chat in the opened chat client, it theoretically cannot use these messages as evidence, but it is technically unavoidable that these messages are also accessed. The problem is that in the moment when the screen appears, the given chat message becomes "read," without the user actually having read it. In such cases the police documents that "when the screen was opened, that window could be seen." This means that no special authorisation is needed to access these "visible" messages and to use them in the criminal proceedings, as they are considered "delivered." It is another matter that during the proceedings this evidence may be contested by the accused or their legal representative on the grounds that they did not actually know the content of that message. With respect to this, the court may decide to exclude the given message from evidence.

e) Injunction to preserve data stored in an information technology system

In relation to an injunction to preserve data stored in an information technology system, the data is also left in the possession of the owner or manager (Section 316 new CP Act). This may be needed, if a larger amount of data has to be examined, but it is not practical to seize the whole system, or it cannot be determined what part of the data should be seized. The new CP Act does not regulate this coercive measure (originally introduced by the Act I of 2002) separately, but as a part of the seizure. The difference is that the injunction to preserve the data may only be effective for three months, while the seizure continues until the end of the procedure or until the confiscation. The main feature of this is that it not only extends to instruments of evidence, but also possibly to any data related to the crime.[73] The name of this coercive power until 2013 was "injunction to preserve data recorded by way of a computer system," then under Act CLXXXVI of 2013, it changed to "injunction to preserve data stored in an information technology system." The new CP Act uses the term "injunction to preserve electronic data" (under Section 316), in uniformity with the other modifications of the act, i.e., acknowledging the admissibility of electronic data as an independent instrument of evidence.[74] In practice, advanced

[73] Villányi, J., Az Európa Tanács informatikai bűnözéssel kapcsolatos egyezményéről, Magyar Jog, 2001(8), p. 470.

[74] Dornfeld, L., A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések, Belügyi Szemle, 2018(2), pp. 115–135.

electronic signatures and time stamps are used for the authentication of the preserved data.[75] After the order, the body issuing the order immediately has to start the examination of the data, and this has to be seized by copying into an information technology system or onto another data carrier. The order may only be issued in relation to a person who did not participate in the perpetration of the crime, as it cannot endanger the success of the proceedings.[76] The possible welfare of the person concerned appears emphatically in so far as the person ordered to preserve the data may, with the permission of the ordering entity store it on another data carrier or system, if the preservation seriously disrupted their main activity.

f) Rendering electronic data temporarily inaccessible (internet blocking)

The rendering of electronic data temporarily inaccessible was entered into the CP Act as of 1 July 2013, for the purpose of combatting child pornography.[77] The idea was that it has to be ensured that the data is rendered inaccessible even before the criminal proceedings are concluded. It is admissible, when the proceedings are initiated for a publicly actionable crime, in relation to which electronic data should be rendered permanently inaccessible (Section 77 Criminal Code) and it is necessary to prevent the continuation of the crime. The coercive measure does not apply to the owner of the data, but to the host provider, and failing his cooperation, the electronic communications service provider, who has to take the corresponding action within one day of the court's decision. Other intermediary service providers (e.g., cache providers) may not be ordered to take the same measure (see Section 2 Point 1 E-Commerce Act).

The new CP Act makes a clear distinction between the "temporary removal" and the "temporary blocking of data" (Sections 335–338 new CP Act). In accordance with the new CP Act, temporary blocking of data may also be applied if it is impossible to identify the entity who should be ordered to remove the data, or if such identification would involve disproportionate difficulties (e.g., in relation to cloud services), and if no results can be expected from the request for legal assistance sent to the foreign authority as regards the temporary removal of electronic data, or if this would involve disproportionate difficulties. The basis of the legal debates in relation to coercive powers was that while initially these only applied in cases in-

---

[75] In relation to the use in court, the most important aspect is authentication and proof of the authentication chain. The legal representative will first contest the inaccuracies during the management of evidence. The legal representative may review such in accordance with their right of access to and perusal of documents. The rights of access and perusal of the accused and their legal representative also extend to electronic documents in addition to printed ones.

[76] Curia Pfv. IV.21.941/2012/5.

[77] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

volving child pornography, crimes against the state and acts of terrorism, altogether nine such crimes were stipulated by Act LXXVI of 2015.

The debate was triggered by the potential consequences of online content blocking for the freedom of speech, and also that the database of removal orders may only be accessed by the National Media and Infocommunications Authority and the electronic communications service providers, and therefore there is no social control over this legal institution.[78] It is, however, an even more serious problem that the coercive measure developed to block online child pornography is no longer suitable for its original purpose, as illegal content appears less and less on the open web.[79]

3. Duties to cooperate: production and decryption orders

a) Decryption order

The decryption obligation of electronic communications service providers is provided by the legislation. The new CP obliges each "organisation addressed with a request for data," i.e., the electronic communications service provider, to also decrypt the data: "The organization addressed with a request for data is obliged to restore the encrypted data or the data otherwise made unknowable to its original state before transfer or disclosure, and to make the content of the data known to the body requesting the data provision" (Section 264(3) new CP Act).

Within the framework of secret information gathering, the service provider is also obliged to make sure that during interception, the bodies entitled thereto may be able to access the information encrypted or compressed by the service provider: "If the electronic communications service provider alters, encrypts or compresses the content of the communication initiated or received by the subscriber in any way, the communication shall be understood as the re-altered, decrypted form or that before compression" (Section 6(2) Government Decree No. 180/2004). However, the service provider shall not be obliged to decrypt the communication encrypted by the user.

The modification of the E-Commerce Act which obliges the application service providers to retain the content of the messages encrypted on the server side and not end-to-end, and to transfer them to the body entitled to collect confidential information has been in force since 2016.[80] According to the E-Commerce Act, the application service provider is: "the natural or legal person or other organization

---

[78] Official opinion of HCLU, on the draft law on the temporary rules of the execution of Act C of 2012 on the Criminal Code, and the modification of other legal pieces, 2011, available in Hungarian at https://tasz.hu/files/tasz/imce/2011/tasz_velemeny_20121026.pdf

[79] Dornfeld, L., A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések, Belügyi Szemle, 2018(2), pp. 115–135.

[80] Established by Section 45(3) of Act LXIX of 2016 in force since 17 July 2016.

without a legal personality who or which ensures access to any software or hardware, software application or related services on specific software or web platform to several users by using electronic communications network […].” (Section 2(m) E-Commerce Act).

The modification of the E-Commerce Act includes the online services of international companies available in Hungary under the force of the legislation (Section 2(g) E-Commerce Act).

The service providers offering end-to-end encryption are obliged to retain and transfer the traffic (meta-) data, as well as the content of the messages to the bodies entitled to secret information gathering subject to external authorisation (Section 3/B. E-Commerce Act).

According to the regulation, the service provider should only decrypt the content of the messages if the communication was not carried out end-to-end (such as for example in the case of Signal application) but was carried out through the server of the service provider.[81] When it comes to compliance with the constitutionality test, the regulation would fail the test of adequacy on this basis, as criminals and terrorists are highly likely to use the applications with end-to-end encryption, in which case the service provider has no decryption obligation.

This provision may have been prompted by the terrorist attack in San Bernardino in 2015 when the NSA was not able to crack the iPhone of the suicide bombers and the service provider did not help them to do so. The case where one of the employees of Facebook was arrested in Brazil because Facebook refused to decrypt a WhatsApp message also happened in the same period. In the same period, a bill was proposed in the United Kingdom which would have forbidden the use of applications using anonymous and encrypted message exchange. However, the Hungarian legislation does not follow this radical approach. The first idea of the Hungarian legislator was very bold, e.g., the use of applications allowing end-to-end encrypted communication (e.g., Signal) would have been declared a criminal offence. However, there was a considerable retreat from this position. There was a version which would have obliged service providers to retain the content of the end-to-end encrypted communication, but finally, the introduction of the decryption of non-end-to-end encrypted messages remained, which was introduced in 2016.[82]

The regulation concerning application service providers could only apply to electronic communications service providers, if they provided a chat service themselves. At the moment, the communications service provider does not have decryp-

---

[81] Dornfeld, L., A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések, Belügyi Szemle, 2018(2), pp. 115–135.

[82] Official opinion of HCLU, on the draft law on the modification of certain legal pieces related to the actions against terrorism, 2016, available in Hungarian at https://tasz.hu/files/tasz/imce/a_tasz_allaspontja_a_terrorizmus_elleni_fellepessel_osszefuggo_egyes_torvenyek_modositasarol_szolo_torveny_tervezeterol.pdf; Máté Szabó, interview.

tion obligations in terms of the content of the communications carried out within the framework of the so-called Over The Top (OTT) application services which use their system. This could be eliminated if the OTT application service provider concluded a contract with the electronic communications service provider for the use of its infrastructure. The other option is for the electronic communications service provider to create their own applications and to allow the users contracted with them to use *only* the applications offered by them through the mobile internet service. In this case the service provider would be able to meet their lawful interception and data retention obligations in terms of the applications offered by them, i.e., the decryption obligation relating to the communications carried out in the application would apply to these as well. As long as the applications are not created, and the downloading thereof is not subject to exclusive user rights, there is neither technical nor legal possibility for this.[83]

b) Self-incrimination

The witness shall say nothing but the truth, but the person accused of a crime and the family member thereof is not obliged to accuse himself or their family member of a crime (or give information relating to it), and thus may not be obliged to decrypt the data encrypted by them or to provide the investigating authority with the decrypting code (Section 85(1)–(3) old CP, Section 179 new CP).

IV. Use of Electronic Communications Data in Judicial Proceedings

1. Intercepted data obtained from outside the criminal justice system

The dilemma is caused by the fact that the scope of the data which is acquired simply through open data acquisition by the investigating authority and that of the intercepted data is intertwined. After applying the secret information gathering tool, a summary report shall be written, and this shall be the subject of the criminal proceeding. This forms part of the investigation documentation which may be known to the accused and their defender. The prosecutor then offers the possibility of concluding an agreement to the defence or takes the matter to the court. Thus, the document presentation obligation extends to the data gathered in a secret manner.

According to the main rule of the criminal proceedings, the parties appearing before the court shall be given the possibility to tell the court what happened in their own words. The evidence shall have a probative value if the court is convinced of

[83] Hungarian Telekom, interviews.

its probative value, established its admissibility, the rights of the defence have been respected and the court finds that the evidence was acquired lawfully.

All data acquired during an open investigation can be used in the criminal proceedings brought in the subject of another crime or against another person. The problem of "usability for different purpose" emerges in the case of secret information gathering (data acquired through interception). Both the old CP and the new CP Act (Sections 256–260) give solutions to this. As it is an activity subject to authorisation (authorised by the judge or the prosecutor), it can be used for the purpose defined in the authorisation, and against the person defined in the authorisation. In addition, it can also be used against a person who is not named by the authorisation, but it turns out later that they can also be accused of the crime. The evidence thus acquired can be used to prove a crime which was not originally named by the authorisation, but which was committed by the target person. One version was omitted from the old CP Act, namely that the data acquired during the secret information gathering could be used to prove a crime not named in the authorisation committed by a person not named in the authorisation; this was therefore not allowed by the old regulation. However, this is permitted under the new CP Act (Section 259) but only if this individual use is authorised by a judge, and only in the case of prioritised, serious crimes (offences against life). The authorisation procedure has to be carried out within a "short term" in every case.

What does "short term" mean? If in the procedure concerning the secret information gathering any item of data arises which indicates a crime, it has to be reported "without delay" in order to begin the criminal procedure. The phrase "without delay" is flexible enough but at the same time it is also uncertain; the old CP did not define what it meant specifically. Many problems arose from this; the use of data thus acquired as evidence was contestable under the criminal procedure (the defender could object that the crime was not reported immediately). This was problematic because the insertion of an item of data into a set of data and its comparative analysis with other data took longer. This was particularly the case when the NSSS acquiring the data did not interpret the item of data after acquiring it (only executes) but transferred it to the client, the investigation authority, and the data analysis was carried out by the latter. At the beginning of the procedure for secret information gathering, when there is hardly any information, the data indicating a crime is not noticeable. However, if data indicating a crime comes to light and the reporting does not take place "without delay," the particular data shall be excluded from the evidence. The point here is that during the surveillance (data interception not for law enforcement purposes) an item of data indicating crime may become apparent, which can be used in the criminal prodedure, but only in the framework of the "evidence admission procedure" defined in the CP Act. The new CP regulates this in the same way as the old one, but omits the adverb "without delay" and operates clearly on a 30-day limit: "The result of the secret information gathering subject to external authorization carried out on the basis of the act on National Se-

curity Special Service can be used in the criminal proceeding if (a) it is intended to be used to prove a crime due to which the use of the secret tools subject to judicial authorization according to this law may be appropriate, and (b) after acquiring the item of data intended to be used in the criminal proceeding the National Security Special Service carrying out the collection of secret information, and the anti-terrorism body of the police initiated the criminal proceeding within thirty days after obtaining the item of data to be used in the criminal proceeding" (Section 260(1)(b) new CP Act). An exception to this is the case where the prior initiation of the criminal proceeding would threaten the successfulness of the task of the body carrying out the secret information gathering; in this case the reporting may take place within one year of acquiring the data (Section 260(2) new CP Act).

2. The right of the accused to object to the use of the evidence

The accused can object to the use of the evidence acquired through interception but may not contest that the tool through which it was recorded has probative value. It is of importance here whether the data was recorded in private premises or in a public space. If you are on the phone while walking in the street and intercepted with a tool placed in the public space, it is not considered as a targeted interception, and on this basis the accused can object to the evidence.

3. Formal requirements to introduce intercepted material as evidence

After carrying out the authorisation procedure, the data acquired through interception can be used with the same formal requirements in the criminal proceedings as if it had been acquired in an open procedure.

V. Exchange of Intercepted Electronic Communications Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

1. International conventions

Within the framework of the legal assistance for evidence acquisition, the transfer of electronic data can be requested in the same way as the transfer of other evidence, and it has to be authorised in the same way as the transfer of the evidence acquired in a secret investigation.

Each of the international conventions relating to cooperation in criminal matters has been signed by Hungary. The norms of the European Union are thoroughly

implemented in Hungary: separately for police / policing and prosecution / enforcement.

On the basis of Act XXXVIII of 1996 on International Legal Assistance in Criminal Matters, Hungary provides legal assistance in criminal matters on a broad scale even without international treaties. Section 6(3) of the Act names the forfeiture of assets or the transfer of the execution of the forfeiture or the assignment thereof as a form of legal assistance in criminal matters which Hungary can fulfil on the basis of an obligation set out in an international treaty. The requests for procedural legal assistance are received by the Chief Public Prosecutor, according to Section 61(2).

The traffic of legal assistance and cooperation in criminal matters between the Member States of the European Union is regulated in Hungary by the legal instruments of the EU and Act CLXXX of 2012 on the cooperation with the Member States of the European Union in criminal matters. Chapter IV of this Act transposed the European Investigation Order (EIO) Directive,[84] which applies to the transfer of electronic data between the Member States of the EU. The judicial authorities (court, prosecutor's office) have the competence to issue and execute the European Investigation Order. In the case of this form of cooperation, the Ministry of Justice does not act as a central authority, and does not have the procedural right to issue or execute the European Investigation Order.

– *2014/41/EU – European Investigation Order (EIO)*

The European Investigation Order (EIO) Directive entered into force in Hungary on the 23 May 2017[85] – without additional legislation.[86]

– *Convention on Mutual Assistance in Criminal Matters (2000)*

In Hungary it was published in Act CXVI of 2005 on the Promulgation of the Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union dated 29th May 2000 and the amending minutes on the publication dated 16th October 2001. The research did not reveal any data on the practical completion of the provisions of Articles 17–21 of the Convention and the problems relating thereto.

– *European Convention on Mutual Assistance in Criminal Matters of 1959*

In Hungary this was published by Act XIX of 1994 on the publication of the European Convention on Mutual Assistance in Criminal Matters done at Strasbourg

---

[84] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32014L0041&from=HU

[85] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order issued in criminal matters.

[86] https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120

dated 20 April 1959 and the additional minutes thereof. The research did not reveal any data on the practical compliance with the provisions of CoE Committee of Ministers Recommendation No. R(85) 10[87] and the problems relating thereto.

– *CoE Convention on Cybercrime (2001)*

In Hungary this was published by Act LXXIX of 2004 on the publication of the Council of Europe Convention on Cybercrime dated 23 November 2001 in Budapest. Parties cooperate on the broadest scale possible during the investigations and proceedings in the matter of crimes relating to computer-related systems and data and in order to collect electronic evidence relating to any crime by applying the international treaties relating to international cooperation in criminal matters and the agreements based on uniform or mutual legal regulations, and their national rights (Art. 23). If the addressing and addressed state is not part of an international agreement, the procedure relating to legal assistance can be still carried out (Art. 27), in Hungary through the International Law Enforcement Cooperation Centre (hereinafter: ILECC). The ILECC was founded in Hungary on the basis of Article 35 of Title III of the Convention, in 2002. The ILECC is part of the 24/7 network set out by the Convention, through which the expedited preservation of the stored computer data (Art. 29), the expedited disclosure of preserved traffic data (Art. 30), and the mutual legal assistance accessing the stored computer data (Art. 31) are possible.

– *United Nations Transnational Organized Crime Convention (2000)*

In Hungary this was published in Act CI of 2006 on the publication of the United Nations Convention against Transnational Organized Crime dated 14 December 2000, signed in Palermo. The role of the central body named in Article 18 of the Convention, which coordinates the completion of mutual legal assistance is also filled by ILECC.

– *Further multilateral international treaties in the field of criminal law*[88]

– Convention on the Surrender for the Execution of the Domestic Punishment of Sentenced Persons signed on 19 May 1978 in Berlin (Decree Law No. 26 of 1979)
– European Convention on the Transit of Sentenced Persons signed on 21 March 1983 in Strasbourg (Act XX of 1994) (Law on enforcement: 9/1995 (III.8.) Decree of the Ministry of Justice)
– European Convention on Extradition signed on 13 December 1957 in Paris (Act XVIII of 1994)

---

[87] https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Rec_1985_10.pdf

[88] Source: Website of the Ministry of Justice, https://goo.gl/y6c7EA

- With the states below the European Arrest Warrant shall be applied (Act CLXXX of 2012): Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, the United Kingdom, Estonia, Finland, France, Greece, the Netherlands, Croatia, Ireland, Poland, Latvia, Lithuania, Luxembourg, Malta, the Federal Republic of Germany, Italy, Portugal, Romania, Spain, Sweden, Slovak Republic, Slovenia
- European Convention on the Suppression of Terrorism signed on 27 January 1977 in Strasbourg (Act XCIII of 1997)
- Criminal Law Convention on Corruption signed on 27 January 1999 in Strasbourg (Act XLIX of 2002)
- European Convention on Laundering, Search, Seizure, and Confiscation of Proceeds from Crime signed on 8 November 1990 in Strasbourg (Act CI of 2000)
- Council of Europe Convention on the Prevention of Terrorism signed on 16 May 2005 in Warsaw (Act II of 2011)
- Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism signed on 16 May 2005 in Warsaw (Act LXIII of 2008)
- Council of Europe Convention on Action Against Trafficking in Human Beings signed on 16 May 2005 in Warsaw (Act XVIII of 2013)
- Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the UN Convention against Transnational Organized Crime, adopted by the United Nations on 14 December 2000 in Palermo (Act CII of 2006)
- Protocol Against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime adopted by the United Nations on 14 December 2000 in Palermo (Act CIII of 2006)
- Protocol adopted on 31 May 2001 Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Amunition, supplementing the United Nations Convention Against Transnational Organised Crime adopted by the United Nations 14 December 2000 (Act XLVIII of 2011)
- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances signed on 20 December 1988 in Vienna (Act L of 1998)
- United Nations Convention against Corruption signed on 10 December 2003 in Merida (Act CXXXIV of 2005)
- International Convention for the Suppression of the Financing of Terrorism of the 54th Session of the General Assembly of the United Nations signed on 9 December 1999 in New York (Act LIX of 2002)

2. Bilateral treaties on mutual legal assistance

Bilateral conventions in criminal matters usually do not contain an exhaustive list of the individual cooperation forms, instead they regulate the main cases of the procedural legal assistance at most in an illustrative manner.[89]

The cooperation with other states in criminal matters is ensured on a broad scale by the bilateral and multilateral international treaties and Act XXXVIII of 1996 on international legal assistance in criminal matters (ILACM) and the legal instruments of the EU within the European Union. The provisions of Act CLXXX of 2012 on the cooperation between the Member States of the European Union in criminal matters (EU CP) have to be applied in relations between the Member States of the EU, unless otherwise provided by the bilateral or multilateral international treaties of the Member State. The ILACM shall be used unless an international treaty concluded within the framework of either the Council of Europe or the EU provides otherwise. The provisions of the international treaty mutatis mutandis do not contain detailed rules concerning which Hungarian authority's competence the enforcement of the provisions should be carried out by and what procedures should be followed during the enforcement of the provisions. The international treaties are published in Hungary by an act; the provisions of Act L of 2005 (Nsztv.) on the procedure concerning international treaties apply. Without an international treaty, cooperation in criminal matters is possible on the basis of reciprocity (in relation to cooperation between the Member States of the EU this term is used for mutuality), without reciprocity the execution of a request for legal assistance (extradition, surrender or takeover of the criminal proceeding, transfer or assignment of the execution of a custodial sentence or detention order, procedural legal assistance), if other conditions are met, is decided upon by the responsible Minister of Justice or the Chief Public Prosecutor in agreement with the minister of external affairs.

The appropriate authorisation for the request for legal assistance depends on the stage of the procedure. If the criminal proceeding has reached the judicial stage, the Minister of Justice will authorise the request for legal assistance, if it is at the police or prosecution stage, it is the Chief Public Prosecutor who will give the authorisation. The competent, executing police authority is also appointed by the authoriser. The ILECC does not execute legal assistance but in urgent cases it forwards it, while the legal assistance is executed by the judicial channel, the ILECC is the body of the police cooperation. (ILECC forwards 10 to 15 such urgent requests for legal assistance a year.) The ILECC executes information and data exchange in police cooperation. The information exchange carried out through police cooperation is not equal to legal assistance.

---

[89] Source: Website of the Ministry of Justice, goo.gl/pNuS4Y

According to the ILACM the forms of the legal assistance in criminal matters are the following: (a) extradition, (b) transfer and takeover of criminal proceeding, (c) takeover or transfer of custodial sentence or detention order, (d) takeover or assignment of the execution of confiscation of assets, confiscation or punishment or action with similar effect (hereinafter: confiscation of assets or confiscation), (e) takeover or assignment of the rendering of electronic data definitively inaccessible or the punishment or action with similar effect (hereinafter: rendering electronic data definitively inaccessible), (f) procedural legal assistance, (g) making denunciation in a foreign state. Legal assistance in criminal matters is executed or requested by the Minister or the Chief Public Prosecutor. According to Section 2 ILACM a request for legal assistance cannot be granted or submitted if it undermines the sovereignty of Hungary, threatens the security, or is contrary to the public order thereof. Unless the ILACM provides otherwise, *the request for legal assistance can be granted or submitted* if (a) the act is punishable according to the law of both Hungary and the foreign State; (b) the legal assistance does not refer to a political crime or any other crime closely related thereto and does not concern a military crime. According to the main rule, the rules of the material law and the procedural law shall be applied to the criminal proceeding even if the criminal proceeding has a cross-border aspect.

Apart from the legislation detailed above, there are no specific regulations or guidelines as to how the interception of the cross-border electronic data or telecommunications data and the transfer of the data has to be carried out.

B. Requirements and Procedure (Including the Handling of Privileged Information)

1. The transfer of electronic data between the Hungarian and foreign authorities – overview

The ILECC belonging to the organisation of the police as a "single window" national contact point carries out each international-level information exchange, which is regulated by Act LIV of 1999 on the cooperation and information exchange realised within the framework of the Law Enforcement Information System of the European Union and the International Criminal Police Organization (hereinafter: ILECC Act). Apart from the ILECC, information exchange is carried out through three main channels: the first is Interpol cooperation, which is also regulated by the ILECC Act (Section 4), the second is the SIRENE communication (SIRENE stands for Supplementary Information Request at the National Entries; SIRENE Act: Act CLXXXI of 2012 on the information exchange within the framework of the second generation Schengen Information System, and the modification of certain acts in the matter of policing relating thereto and the Magyary Simplification Programme), the third is the Europol communication channel

(Act CLXXX of 2012 on the cooperation with the Member States of the European Union in criminal matters, a.k.a. the Europol Act) – the numbering does not indicate a rank or hierarchy of the communication.

SIENA (the Secure Information Exchange Network) is the communication system of Europol, which has been used by the end users since 1 August 2017, i.e., by the regional and local autonomous bodies (county police headquarters, Budapest Police Headquarters, National Investigation Bureau, National Tax and Customs Administration, National Security Special Service, Counter Terrorism Centre, and the Anti-Terror Information and Criminal Analysis Centre in order to control passenger traffic) on a mandatory basis (the 25/2017. (VIII. 17.) National Police Headquarters instruction on the execution of the joint order of the cooperation and information exchange implemented by using the applications of the European Security Network operated by the European Police Office 23/2016. (IX. 15.) of the Ministry of Interior Affairs and the Ministry for National Economy). Through the SIENA system the exchange of the data obtained both in open and secret investigation is carried out. Thanks to the end-to-end user authorisation development of SIENA the ILECC's workload has diminished. The communication between the border policing bodies of each country is also carried out through the Common Contact Points but only in terms of the user's basic data (e.g., checking the owner of the vehicle, personal details). Although the above-mentioned authorities have end-user licences to obtain data through the SIENA system, the ILECC has to be notified of all of these data transfers subsequently.[90]

The information passing through the channel of ILECC facilitates the work of the police. The ILECC can be a channel in all cases in which the acting police headquarters do not have a direct foreign partner. This extends from the execution of the simplest operations ("prioritisation" or the so-called criminal history check, dactyloscopy information, etc.) to the most complicated ones (extradition, organisation, and execution of the handover of evidence). If a cooperation agreement is in force with the service provider (this applies to most of the large telecommunications service providers), ILECC carries out the request for telecommunications data and those from the internet service providers. If no such cooperation agreement is in force, the request for data can be executed by reference to the CP Act. This applies to smaller telecommunications service providers. ILECC facilitates the requests for data both from the domestic and foreign service providers. Therefore, it is the ILECC that provides assistance for the handover and takeover of the telecommunications data, i.e., the transfer of data abroad and from abroad.

---

[90] ILECC, interview.

2. Urgent request by foreign State for criminal cooperation

There are three types of deadlines in the case of requests sent out by ILECC: (a) immediate request (very urgent / flash): to be executed by the afternoon of the same day or by the start of the next business day, (b) urgent request: by the end of the second day from the receipt of the request or by the start of the third day, and (c) normal: with a completion deadline of 30 days. If the request through ILECC would result in a delay threatening the success of the cooperation, the Hungarian cooperating body shall contact directly the body established for the international cooperation in criminal matters and the national units thereof. The concerned Hungarian cooperating body shall notify ILECC of the contact and the request within 48 hours (Section 3(1)(a) ILECC Act).

3. Problems arising in practice

Problems can arise from the execution of the request by foreign service providers, and the source of the problem might be legislative or technical.[91]

a) Legislative problems

Since the legislation of certain countries sets different deadlines for the retention, handling, and handover of the data, there is a high degree of variation in the granting of requests by foreign service providers: some hand over the requested item of data within the framework of a legal assistance procedure and some via a simple Interpol information exchange. This can be important as concerns timing, since information exchange within the framework of legal assistance is much slower[92] than that which is based on informal connections:

– The foreign service providers disclose IP addresses and other traffic data only within the framework of a legal assistance procedure.
– There is a list containing the countries which will release the subscriber's data in a legal assistance procedure and which will use the Interpol channel (e.g., Austria and Germany make the data available directly, outside the legal assistance procedure, while Romania and the USA do not; it varies whether the United Kingdom acquires the data outside the legal assistance procedure or not).[93] This

---

[91] ILECC, interview.

[92] The request for legal assistance has to be translated and presented, if it is received by the foreign authority, it has to be translated there as well, forwarded to the executing body, then the answer has to be re-translated, etc. All together the execution of the request for legal assistance takes 2 to 6 months. In comparison, the information exchange carried out through ILECC takes 2 days on average. See the 3 urgency categories.

[93] For the execution of the request addressed to Great Britain, a 3-page questionnaire has to be filled in; the request for data has to be well justified as the local liaison pays for the requested data to the service provider (how the requested item of data will facilitate the

depends exclusively on the internal rules of the given country; the regulations of the Member States vary enormously within the EU.[94]

– The regulation of the data considered to be banking secrets is similarly variable according to Member States, and it can be different according to financial institutions within each Member State (e.g., the United Kingdom). Other countries (e.g., Germany, Austria) do not disclose data considered as banking secrets except in the case of a request for legal assistance. In these countries not only the law, but also the Constitution protects banking secrets, so the service provider may not disclose them on a foreign request.
– As in Germany the prepaid service is anonymous, the user data is not recorded. Although in Hungary there is a rule that provides that the user has to be named even in the case of prepaid services, there is still a lot of fraud; homeless people have more than 1,000 such subscriptions and use such cards to commit minor crimes. An example of this was the service provider in Hungary named Bencso-Tel Ltd. purchasing several 100,000 such prepaid subscriptions but they did not have to keep a record on who they sold them to, so they were not able to follow the actual users. In another case related to human trafficking, 99 % of the used phone numbers led to telecommunications service providers and homeless people, so it could not be established who was using the phones when the crime was committed. This meant a deadlock for the investigation, and they had to acquire more information on other strands. In a third case of a burglary committed in Austria, the Austrian authorities requested all the Hungarian phone numbers logging in to the given radio telephone station, the data of the subscribers and their criminal records. It was practice between 2008 and 2011 to send requests for data on such a large scale to the service providers. The Hungarian contact body, the ILECC refused to respond to this type of foreign request, as it did not comply with the principle of purpose limitation. For this reason, these types of requests for data have disappeared.[95]
– A lot of data could be acquired from the service provider operating the server of Gmail. The United States disclose all data within the framework of legal assistance, even if the USA has a Europol contact point in Hague, the telecommunications data cannot be requested on this channel unless a Europol Joint Investigation Team is formed. This is the reason why perpetrators prefer the American

---

investigation, whether there is another possibility to prove, whether it is possible to acquire it in another way, etc. so the complete investigation material has to be described and translated).

[94] In these cases, platforms would be available (e.g., Whois record) which allow the IP range to be consulted. However, it does not provide precise, only approximate information and is not reliable in the case of dynamic IP addresses. Furthermore, from these publicly available databases we can only find out in which country the registered service provider used the given IP range in the given time. Although it is not possible to access personal data from open source, the foreign service provider can be found.

[95] Source of the cases: ILECC interviews.

servers, as they know that it is very difficult and lengthy to acquire telecommunications data from the American service providers. The police of the USA will cooperate, but it is only advisable to apply for legal assistance with them if the direct data request from the service providers is not a viable option.

b) Technical problems

Technical problems occur when the data request concerns internet-based phone services (VoIP). In this case it is necessary to request the dynamic IP addresses, which the users may change every second, so it is necessary to define the time of use precisely to the second which is often impossible.

– No duty to filter out or to delete privileged information before transmitting the results of an interception measure to a foreign country

Telecommunications data does not get the same level of protection as the data considered as bank data, so the service provider is not bound by the duty of filtering. It has to be noted that the complete log file (logging data) of the communication is not handed over by the service provider, only the item of data to which the specific request referred. Therefore, there is no duty of filtering here either. Some issue of data is governed by purpose limitation: the time interval, person, and reason have to be provided in the request.

C. European Investigation Order

1. Legal regulation: Granting and executing foreign requests for the interception of telecommunications

In 2017, new sections were inserted into the act on cooperation with the Member States of the European Union in criminal matters (EU CP) which concern the order of issuing and executing the European Investigation Order (EIO)[96] for the knowledge and recording of the communication forwarded through the electronic communications service, computer tool or system in a secret manner, without being known to the concerned person (Sections 65/A–65/D EU CP).

The EIO for acquiring electronic data is executed by the prosecutor's offices (Chief County Prosecution or Capital Prosecutor's Office), according to the rules of data acquisition with secret tools in criminal proceedings or those of the secret information gathering subject to judicial authorisation. In case of urgency, controlled deliveries or the application of covert investigators can be initiated and granted by the competent director of the police or of the National Tax and Customs

[96] 2014/41/EU – European Investigation Order (EIO); https://www.ejnforum.eu/cp/registry-files/3339/Competent-authorities-and-languages-accepted-EIO-31-May-2018.pdf

Administration, appointed by the relevant law, for the duration of 24 hours, with the immediate notification of the competent public prosecutor, whose subsequent approval is required. When an EIO is issued by a public prosecutor during the investigative phase for a measure that falls under the competence of the investigative judge, the EIO needs to be validated by an investigative judge. If an EIO for an administrative offence is not issued by a court, the EIO will be validated by the Office of the Prosecutor General. EIOs might be transmitted through the secure channels of the European Judicial Network or Eurojust. In cases of legal assistance for administrative offences, the receiving authority is the central authority, which is the Prosecutor General. Hungary has not designated a central authority to issue and execute an EIO. In cases of legal assistance for administrative offences, the central authority is the Prosecutor General. In urgent cases or if the transmission of the EIO in the Hungarian language meets extreme difficulties, English, French, or German language is accepted.

2. Formal requirements

The EIO has to be sent to the prosecutor's offices in Hungary (Capital Prosecutor's Office) by filling in the form included in the Annex of EU CP in English, French, German, or Hungarian. The prosecutor shall inform the requesting authority of the Member State within 96 hours of receipt of the EIO if the conditions for executing the request are not met. If the prosecutor or the judge does not authorise the execution of the EIO according to the content of the request, the prosecutor may consult the foreign authority.

The data acquired (recorded) as a result of the execution of the EIO may be transmitted to the Member State either after the completion of the procedural act, or by the result of the surveillance (data) being forwarded directly to the tool of the Member State authority, if the requesting party expressly requests so (request for direct forwarding).

The requesting party may ask at their own expense for the prosecutor to transcript the data or to receive the encrypted item of data restored to its original state (decrypted).

In the EIO it is possible to request classified data (e.g., bank secrets, etc.) and this shall not preclude the transfer of the acquired data (the classification has to be removed if necessary and transferred to the requesting party if there is a legal possibility according to the Act on the Protection of Classified Data.

The prosecutor may issue an EIO for the acquisition of electronic data located in another Member State. If the data can be acquired in several Member States, the EIO has to be forwarded to the Member State which is able to execute it in the most efficient way, which should be the state according to the place of residence of the concerned person, if possible.

3. Contents of the order

In the order the prosecutor specifies the reasons on the basis of which it is assumed that the acquisition of the evidence which is intended to be acquired would be hopeless in any other way, and the form in which the item of data is requested (after recording or by direct forwarding). The prosecutor may request the transcription of the data, or in the case of encrypted data, the release of the encryption (restoration into the original state) and the removal of the classification of the data (for the purpose of transferability). The Hungarian state advances these expenses.

If in Hungary secret information gathering subject to judicial authorisation is conducted against someone, but the person under surveillance does not reside in Hungary, and the assistance of the country of residence of the concerned person is technically not necessary for the surveillance and recording of their communication, the prosecutor shall notify the Member State where the subject resides (through the form included in the Annex of EU CP) (Section 65/D(1) EU CP). If the authority of the Member State informs the prosecutor within 96 hours that according to the national law the secret information gathering cannot be authorised, the prosecutor shall take the necessary measures according to the CP. If the prosecutor does not agree with the standpoint of the Member State, he/she can initiate consultation with the authority of the Member State with the assistance of Eurojust (Section 65/D(3) EU CP).

4. No direct execution

There is no such legislative authorisation according to Sections 65/A–65/D and 69/E–65/H of Act CLXXX of 2012 on cooperation with the Member States of the European Union in criminal matters. According to Section 4(2) of Act XXXVIII of 1996 on international assistance in criminal matters, the legal assistance in criminal matters is executed by the Minister or the Chief Public Prosecutor. Therefore, *direct extraction and transfer* of intercepted electronic communications data among foreign police and judicial authorities is not possible according to the national legal regime.

– The European Investigation Order and the effective mutual legal assistance in light of the transfer of telecommunications data (Sections 69/E–69/H EU CP)

The request for procedural legal assistance for the knowledge or recording of the communications transmitted through electronic communications services or a computer device or system without the knowledge of the concerned person in a secret manner is executed by the prosecutor according to the rules of the criminal proceedings relating to the secret information gathering subject to judicial authorisation (Section 69/E EU CP). Procedural legal assistance can be executed if the authority of the Member State has authorisation according to the law of its own state. If the information gathering in the request can be executed in Hungary within the framework of secret information gathering subject to judicial authorisation, the

investigating magistrate shall make a decision on the request on application by the prosecutor. If the magistrate refuses the request application, the prosecutor shall inform the judicial authority of the Member State. The result of the request for procedure shall be directed to the authority of the requesting state either after the completion of the procedural act (in the form of recorded data) or directly if the technical conditions are met. The prosecutor, on the request of the requesting Member State, may order the transcription of the data in this case, too.

The request for legal assistance relating to the surveillance of a person residing in Hungary is assessed by the Capital Prosecutor's Office according to whether the conditions of the secret information gathering are met in the Hungarian law. The judge shall respond within 96 hours of receipt, but this deadline can be extended by eight days if necessary.

If the person concerned by the criminal proceeding in progress in Hungary does not reside in Hungary, but the assistance of the Member State of their residence is not necessary for the surveillance of their electronic communications, after disclosing the identity of the concerned person the prosecutor informs the Member State of residence without delay. If the Member State informs the prosecutor within 96 hours (or within 12 days if the deadline is extended) of the fact that secret surveillance is not allowed by the national law, or the result of the secret surveillance already executed may not be used or only if specific conditions are met, the prosecutor shall take the necessary measures according to the CP. If the prosecutor does not agree with this, he can initiate consultations with the assistance of Eurojust.

5. Technical, legal and/or organisational modifications needed for real time cooperation

In order for service providers to directly serve the data requests of foreign authorities, a clear and comprehensive legislative background would be necessary. However, state sovereignty, the priority of national security interests, and the role of electronic communications or commercial service providers create barriers to the implementation of real time cooperation.

The European Commission presented on 17 April 2018 the proposed European regulation relating to criminal matters, imposing the obligation of disclosure and retention of electronic evidence[97] (hereinafter: Proposed Regulation) and the proposed directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[98] At the time of the preparation of this re-

---

[97] Proposal: *Regulation of the European Parliament and of the Council* on the European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final – 2018/0108 (COD), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN

[98] Proposal: *Directive of the European Parliament and of the Council* on the definition of the harmonized rules on the appointment of the legal representative for the purpose of

port the development of the standpoint of the Hungarian government concerning these two proposed regulations is still in progress. They were also sent to the companies providing electronic communications service for their opinion through the Communications Reconciliation Council. At the moment, the communications service providers do not have legal authorisation to examine whether there is a legal basis for a request as the authorities of the sovereign states are entitled to do. Such a situation could arise where the European Proposed Regulation provides for the service providers to receive and execute foreign requests directly, while according to the local (national) legislations it is not possible in the given case as the legal base is missing, or the disclosure of the data requested by the foreign authority actually threatens the national security (classified data). Moreover, the communications service provider is a market player, and the examination of the legal base, and the source of the foreign request (whether the issuer has the right to request data) are not part of their range of services; it is currently carried out by the bodies executing requests for mutual legal assistance. The Proposed Regulation would remove the authorities from the execution of the requests for legal assistance and would entrust the service providers to examine the legal base. At the moment, neither the legal, nor the technical conditions for this are met. The lack of official control envisaged by the Proposed Regulation would not be solved by the Annex including the forms on the direct execution of the data disclosing attached thereto.[99]

D. Statistics

Similarly to the data retention rules, the obligation to gather statistical data relating to data requests was included in the E-Communications Act having regard to the Data Retention Directive:[100]

> **Section 159/A(7) E-Communications Act**
> The organizations entitled for request for data by a special law are obliged to make annual statistics and send them to the European Commission. The statistics shall contain the following: (a) the cases where the service provider provided the competent authorities with data according to this Section, (b) the time of the retention of the data according to this Section and the time passed between that and the request of the competent authority for the forwarding of the data, (c) the cases where the service provider was not able to execute the request.

On the basis of the Nbjt. Hungary is able to provide legal assistance in criminal matters even without an international treaty. The requests for procedural legal as-

---

gathering evidence in a criminal proceeding COM/2018/226 final – 2018/0107 (COD), available at https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vknmikug23z1

[99] Hungarian Telekom, interview.

[100] These provisions were established by Section 53 of Act CVII of 2011 effective from 3 August 2011.

sistance are received by the Chief Public Prosecutor according to Section 61(2), so the statistical data relating to the specific cases may be available there.

Legal assistance traffic and cooperation between the Member States of the European Union in criminal matters are regulated by the legal instruments of the EU and the EU CP. Chapter IV of the EU CP transposed the Directive on the European Investigation Order which applies to the transfer of electronic data between the Member States of the EU. The judicial authorities (court, Prosecutor's Office) are competent to issue and execute the EIO. In view of the above, the mentioned bodies may possess the statistical data.

Despite the author's requests, the organisations entitled to request data, i.e., investigation authorities, chief public prosecutor executing the procedural legal assistance, the judicial authorities entitled to issue and execute the European Investigation Order (court, Prosecutor's Office) were not able to provide any statistics.

Only the largest service providers providing communications and commercial services, i.e., Telenor, Hungarian Telekom (latter is the subsidiary of Deutsche Telekom) have transparency reports including named, non-specific data which might give some information in connection with data requests concerning services.

The ILECC does not keep statistics on how many requests are executed by them on an annual basis as they are not authorised to keep such a database. Approximately 3,000 foreign requests are received annually by the Hungarian ILECC. It is not recorded, however, how many of these are related to telecommunications data. It is possible that the case starts with a simple warrant, and later within this framework a request for telecommunications data is received. The case categories are not registered according to crimes either.[101]

Appendix

Case law

Domestic case law

Curia Pfv.IV.21.941/2012/5.

AB IV/03085/2012 Alkotmánybírósági panasz

8/1990 (IV.23.) AB határozat

3038/2014 (III.13.) AB határozat

17/2014 (V.30.) AB határozat

[101] ILECC, interview.

European and international case law

Szabó and Vissy v. Hungary, judgement of 1 December 2016, no. 37138/14

Roman Zakharov v. Russia, judgement of 4 December 2015, no. 47143/06

BVerfG, 1 BvR 370/07

Referred legal rules with abbreviations

Domestic legal rules

Abbreviation	Hungarian name	English name and abbreviation, if available
180/2004 Korm.r. / Government Decree No. 180/2004	180/2004. (V. 26.) Korm. Rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről	Government Decree No. 180/2004 (V.26.) Decree on the rules of cooperation on electronic communication organisations and organisations authorised to perform secret information gathering and secret data interception (Government Decree No. 180/2004)
Alaptörvény / Constitution	Magyarország Alaptörvénye (2011. április 25)	Fundamental Law, 25 April 2011
Be., old	1998. évi XIX. Törvény a büntetőeljárásról	Act XIX of 1998 on the criminal procedure, old CP Act
Be., new	2017. évi XC. Törvény a büntetőeljárásról (hatályos 2018. Július 1-től)	Act XC of 2017 on the criminal procedure (effective from 1 July 2018), new CP Act
Btk. / CC	2012. évi C. törvény a büntető törvénykönyvről	Act C of 2012 on the Criminal Code
Bvtv.	2013. évi CCXL. Törvény a büntetések és intézkedések végrehajtásáról	Act CCXL of 2013 on the execution of penal sanctions and measures
Egtv.	1997. évi XLVII. Törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről	Act XLVII of 1997 on managing and protecting of health related personal data
Eht. / E-Communications Act	2003. évi C. törvény az elektronikus hírközlésről	Act C of 2003 on electronic communications (E-Communications Act)
Ekertv. / E-Commerce Act	2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről	Act 100 of 2003 on certain issues of electronic commerce activity and on information society (E-Commerce Act)

EUbe. / EU CP	2012. évi CLXXX. törvény az Európai Unió tagállamai közötti bűnügyi együttműködésről	Act CLXXX of 2012 on the cooperation between the Member States of the European Union in criminal matters (EU CP)
Europol tv. / Europol Act	2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről	Act CLXXX of 2012 on the cooperation with the Member States of the European Union in criminal matters (Europol Act)
Infotv. / Info Act	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról	Act CXII of 2012 on informational self-determination and the freedom of information (Info Act)
Könyvtv.	2007. évi LXXV. Törvény a Magyar Könyvvizsgálói Kamaráról, a könyvvizsgálói tevékenységről, valamint a könyvvizsgálói közfelügyeletről	Act LXXV of 2007 on the auditing services
Mavtv.	2009. évi CLV. törvény a minősített adat védelméről	Act CLV of 2009 on the protection of classified data
Navtv. / Tax Authority Act	2010. évi CXXII. Törvény a Nemzeti Adó- és Vámhivatalról	Act CXXII of 2010 on the national tax and customs administration (Tax Authority Act)
Nsztv.	2005. évi L. törvény a nemzetközi szerződésekkel kapcsolatos eljárásról	Act L of 2005 on the procedural rules regarding international treaties
Nbtv. / NSSA	1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról	Act CXXV of 1995 on the National Security Services (NSSA)
Nbjtv. /ILACM	1996. évi XXXVIII. Törvény a büntetőügyekben más államokkal folytatott együttműködést a két- és többoldalú nemzetközi szerződések és a nemzetközi bűnügyi jogsegélyről (Nbjtv.)	XXXVIII of 1996 on international legal assistance in criminal matters (ILACM) Act
NEBEK tv. / ILECC Act	1999. évi LIV. törvény az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről	Act LIV of 1999 on the cooperation and information exchange realized within the framework of the Law Enforcement Information System of the European Union and the International Criminal Police Organization (ILECC Act)
Ptv.	2017. évi LIII. Törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról	Act LIII of 2017 on hindering money laundering and financing terrorism
Ptk.	2013. évi V. törvény a polgári törvénykönyvről	Act V of 2013 on the Civil Code
Pp.	2016. évi CXXX. Törvény a polgári perrendtartásról	Act CXXX of 2016 on the civil procedure

Rtv. / Police Act	1994. évi XXXIV. Törvény a rendőrségről	Act XXXIV of 1994 on the police force
SIRENE tv. / SIRENE Act	2012. évi CLXXXI. Törvény a Schengeni Információs Rendszer második generációja keretében történő információcseréről, továbbá egyes rendészeti tárgyú törvények ezzel, valamint a Magyary Egyszerűsítési Programmal összefüggő módosításáról	Act CLXXXI of 2012 on the information exchange within the framework of the second generation Schengen Information System, and the modification of certain acts in the matter of policing relating thereto and the Magyary Simplification Programme (SIRENE Act)
Üvtv.	2017. évi LXXVIII. Törvény az ügyvédi tevékenységről	Act LXXVIII of 2017 on the activities of attorneys
Ütv.	2011. évi CLXIII. Törvény az ügyészségről	Act CLXIII of 2011 on the public prosecution

International legal rules and their publications in Hungary

English name with abbreviation, if available	Hungarian name
Act XIX of 1994 on the publication of the European Convention on the Mutual Assistance in Criminal Matters (*European Convention on Mutual Assistance in Criminal Matters of 1959*)	1994. évi XIX. Törvény a Strasbourgban, 1959. április 20-án kelt, a kölcsönös bűnügyi jogsegélyről szóló európai egyezmény és kiegészítő jegyzőkönyvének kihirdetéséről
Act LXXIX of 2004 on the publication of the Council of Europe Convention on Cybercrime (*CoE Convention on Cybercrime 2001)*	2004. évi LXXIX. Törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről
Act CXVI of 2005 on the Promulgation of the Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union (*Convention on Mutual Assistance in Criminal Matters 2000)*	2005. évi CXVI. Törvény az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről szóló, 2000. május 29-én kelt egyezmény és az egyezmény 2001. október 16-án kelt kiegészítő jegyzőkönyve kihirdetéséről
Act CI of 2006 on the publication of the United Nations Convention against Transnational Organized Crime (*United Nations Transnational Organized Crime Convention 2000)*	2006. évi CI. Törvény az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény kihirdetéséről

Bibliography

Bejczi A. (2012). Célpontban a megbízhatósági vizsgálat, Belügyi Szemle 60(6): 24–65.

Bezsenyi T. (2015). A szervezett bűnözés elleni nemzetközi együttműködés értelmezési a magyar igazságszolgáltatásban, Polgári Szemle, 11(1-3); http://old.polgariszemle.hu/?view=v_article&ID=671

Brenner, S.W. (2011). Budapesti law – A United States perspective, in: E. Casey (Ed.) Digital Evidence and Computer Crime, Academic Press, pp. 115–118.

Data Privacy Commissioner (2009). A nemzetbiztonsági szolgálatok külső engedélyhez kötött titkos információgyűjtéséről szóló adatvédelmi biztosi ajánlás, Ügyszám:1813/T/2008-4., http://abi.atlatszo.hu/index.php?menu=aktualis/ajanlasok&dok=1813_T_2008-4

Detrekői Zs. (2014). Blokkolás Magyarországon – hogyan jutottunk el a gyermekpornográfia elleni küzdelemtől a szerencsejáték-oldalak blokkolásáig? Infokommunikáció és Jog, 2014(60): 185–187.

Dornfeld L. (2018). A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések, Belügyi Szemle, 2018(2): 115–135.

EKINT (2017). Az Eötvös Károly Intézet álláspontja a nemzetbiztonsági célú titkos információgyűjtés független felülvizsgálatáról szóló törvénytervezetről, http://www.ekint.org/maganszfera-adatvedelem/2017-08-24/allaspont-a-nemzetbiztonsagi-titkos-megfigyelesrol-szolo-tervezetrol

Finszter G./Korinek L. (2018). Az eltűnt gyanú nyomában, Belügyi Szemle 2018(3): 104–122.

Gaiderné Hartmann T. (2015). Az elektronikus adatok ideiglenes és végleges hozzáférhetővé tétele – egy új intézmény első évei, Magyar Jog, 2015(2): 109.

HCLU (2011). A Társaság a Szabadságjogokért véleménye a Büntető Törvénykönyvről szóló 2012. évi C. törvény hatálybalépéséhez kapcsolódó átmeneti rendelkezésekről és egyes törvények módosításáról szóló törvénytervezetről, https://tasz.hu/files/tasz/imce/2011/tasz_velemeny_20121026.pdf

HCLU (2016). A Társaság a Szabadságjogokért álláspontja a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló törvény tervezetéről. https://tasz.hu/files/tasz/imce/a_tasz_allaspontja_a_terrorizmus_elleni_fellepessel_osszefuggo_egyes_torvenyek_modositasarol_szolo_torveny_tervezeterol.pdf

HCLU (2017). Vélemény a Belügyminisztérium nemzetbiztonsági szolgálatokról szóló törvény és az információs jogi törvény módosításával kapcsolatos, BM/8652/2017. Számú előterjesztéséről, https://tasz.hu/files/tasz/imce/2015/nbtv_velemeny.pdf

HCLU (2018). A transparency report-ok összeállításáról és nyilvánosságra hozataláról emberi jogi szemszögből, https://tasz.hu/a/files/Transparency-Report-kezikonyv.docx

Kasznár A. (2018). A kibervédelem fontossága a terrorelhárítás jelenlegi és jövőbeni rendszerében, Belügyi Szemle 2018(2): 106–114.

Laczi, B. A szamitogep es a buntetojog. Magyar Jog 2001(3), pp. 137–152.

Lakatos A.A. (2017). Az informatikai bűncselekmények és a Bitcoin, Belügyi Szemle, 2017(1): 29.

Mező I. (2009). Személyes adatok védelme az Európai Unió jogában és Magyarországon, PhD értekezés, Miskolci Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskola, http://midra.uni-miskolc.hu/document/5522

Miskolczi B. (2017). A kényszerintézkedések új rendszere, Jogász/Világ, 2017. február 21., https://jogaszvilag.hu/rovatok/szakma/a-kenyszerintezkedesek-uj-rendszere

Sorbán K. (2016). Digitális bizonyíték a büntetőeljárásban, Belügyi Szemle 2016(11): 81

Sulyok M. (2017). A bizalmi kapcsolattartás bizonyítási védelme a magyar polgári eljárásban – alkotmányjogi szempontok, Eljárásjogi Szemle, 2017(2): 1–30.

Szabó M./Hídvégi F. (2014). Két ítélet és végrehajtásuk. Az Európai Bíróságnak az adatvédelmi biztosról és az adatmegőrzésről szóló ítéletei és azok utóélete Magyarországon, Fundamentum, 2014(4): 72–74.

Szathmáry Z. (2015). Az elektronikus pénz és a Bitcoin biztosítása a büntetőeljárásban, Magyar Jog, 2015(11): 639–641.

Tóth F. (2017). Az informatikai bűnözéshez kapcsolódó kényszerintézkedések, Büntetőjogi Szemle, 2017(1): 79.

Vadász, V. A szamitogep demisztifikalasa. Ugyeszek Lapja 2010(2), pp. 13–21.

Villányi J. (2001). Az Európa Tanács informatikai bűnözéssel kapcsolatos egyezményéről, Magyar Jog, 2001(8): 470.

Vissy B. (2016). Az információs önrendelkezési jog, előadás, ELTE ÁJK Alkotmányjogi Tanszék, 2016. november 28.

Italy*

National Rapporteurs:
Roberto Flor
*Stefano Marcolini***

* This report reflects legislation and case law as of October 2018.

** Roberto Flor (Sections III.C.–V.); Stefano Marcolini (Sections I.–III.B.).

Contents

I. Security Architecture and the Interception of Telecommunications

A. Law Enforcement Institutions and Security Services with Powers of Telecommunications Interception

1. National security architecture

In all Western countries, Italy included, the fight against crime has two faces. On the one hand, the main public duty is to investigate and identify the people responsible for criminal activities and to impose a sanction upon them. On the other hand, the State is required to adopt preventive policies and protect its own citizens from future crimes that are yet to be committed.

According to the functions respectively attributed by the Italian Code of Criminal Procedure (*codice di procedura penale*, CPP), the public prosecutor *(pubblico ministero)* and or the judge have the competence for the investigation, ascertainment, and punishment of individuals responsible for crimes that have already been committed. It is worth noting that in Italy both the judge and the public prosecutor belong to the judicial order, which is autonomous and independent from other state powers. Even though the CPP, introduced in 1988, was inspired by the principles which underpin the adversarial model, the high number of amendments to the CPP over the years have introduced certain ambiguous aspects.

Crime-prevention policies do not stem from the judiciary, but from the executive and the relevant Ministers in light of their competences (while criminally relevant behaviours are defined by the legislature instead).

In Italy there are many different armed forces at the national level. The *Arma dei Carabinieri* reports to the Minister of the Defence and, together with the Army, the Navy, and the Air Force, is part of the Italian Armed Forces. The *Polizia di Stato* fulfils its duties under the supervision of the Minister of the Interior and the *Guardia di Finanza* reports to the Minister of Economics and Finance. It is important to remember that a fourth organ exists, the *Corpo di Polizia Penitenziaria*, which is responsible for the surveillance of Italian detention institutions. Regional and local police forces are of little importance for this report.

The tasks of the police forces are connected both to criminal investigations and preventive measures.

Within criminal investigations, the police forces have the power to arrest in the act, to investigate following directions provided by the judicial authority and also autonomously and, more generally, to aid and support the prosecutor and the judge in their duties. For this reason, the judicial police is usually considered to be “assis-

tant/auxiliary" to the judicial authorities in criminal investigations. Art. 109 Constitution states that "the judicial authorities have direct disposal of the judicial police." It is also important to remember that in an attempt to balance the state powers, the Italian legislator has always refused to create a judicial police force directly dependent on the judicial authority. For this reason the expression "judicial police" in Italy does not describe an organ, but a function.

When dealing with preventive investigations, the police forces act as security forces according to the Government's directives and the statutory law contributing to preventive activities. On the side of "intelligence" preventive investigations, *legge* no. 124 of 3 August 2007 created the *Sistema di informazione per la sicurezza della Repubblica* in order to renew the former secret services apparatus and prepare it for the challenges of a new economic, political, and social context, both nationally and internationally, particularly regarding organised crime and terrorism (the law was then modified in 2009 and 2012).

In the previous system the intelligence agency was subordinate to the Ministries of Defence and of Interior, while after the reform the powers and the connected responsibilities fell to the Prime Minister, who exercises powers through the *Dipartimento delle informazioni per la sicurezza* (DIS). The DIS is an organ acting within the Prime Minister's Cabinet *(Presidenza del Consiglio dei Ministri)*. The statute and organisation of DIS is ruled by a specific decree, the *Decreto del Presidente del Consiglio dei Ministri* no. 2 of 1 August 2008. The decree must be read in conjunction with the *Decreto del Presidente del Consiglio dei Ministri* no. 1 of 12 June 2009. The Prime Minister appoints the director and vice-directors of two new Agencies: *Agenzia informazioni e sicurezza esterna* (AISE) and *Agenzia informazioni e sicurezza interna* (AISI). While AISE is responsible for information regarding threats to national security coming from abroad (for its organisation, see *Decreto del Presidente del Consiglio dei Ministri* no. 3 of 1 August 2008 and *Decreto del Presidente del Consiglio dei Ministri* no. 2 of 23 March 2011), AISI deals with information regarding the internal security of the Republic and the stability of democratic institutions (for its organisation, see *Decreto del Presidente del Consiglio dei Ministri* no. 4 of 1 August 2008). The system is completed by another body, the *Comitato interministeriale per la sicurezza della Repubblica* (CISR), created within the Cabinet of the Prime Minister with consultative and deliberative functions concerning the direction and general scope of security activities.

Besides the *Sistema di informazione per la sicurezza della Repubblica*, there are also military intelligence units within the High Command for the Defence *(Stato maggiore della difesa)*, which collect information in conjunction with AISE in order to protect military bases and the activities of the armed forces abroad.

2. Powers for the interception of telecommunications

a) Law of criminal procedure

i) 'Regular' interceptions are based on arts. 266 ff. CPP. According to this the public prosecutor may ask the pre-trial judge *(giudice per le indagini preliminari)* to authorise the "interception of conversation or communications" (art. 266 CPP) or of "cyber or telematic communications" (art. 266-*bis* CPP) only when related to grave crimes that, due to their nature, require special investigative techniques, or alternatively related to non-serious crimes (such as threats) that are committed by telephone or through cyber- or telematic-means. This is considered to be the "ordinary" interception regime.

In order to grant the prosecutor's request, the pre-trial judge *(giudice per le indagini preliminari)* has to verify the existence of certain requirements. First of all, they must assess whether there is sufficient reason to believe that a crime has been committed (the provision says "serious evidence of crime," *gravi indizi di reato*). Furthermore, interceptions must be "absolutely indispensable for the continuation of the investigations" (art. 267(1) CPP). The judge authorises the interceptions for not more than fifteen days, but the time limit can be extended for fifteen days. The law does not provide an upper limit on such extensions.

ii) Still within the category of the criminal procedural interceptions, more provisions exist. The most important is II) art. 13 of *decreto-legge* no. 152 of 13 May 1991, adopted into law with amendments by *legge n*o. 203 of 12 July 1991.

This provision allows interceptions operations which have only a "sufficient basis/evidence" *(indizi sufficienti)*, even if not "serious." Moreover, it does not require the "absolute indispensability for the continuation of the investigations," but the mere "necessity for the conduct of investigations." Furthermore, it also deals with investigations regarding "organised crimes or phone-threats."

Recently the *Corte di Cassazione* in plenary session elucidated the meaning of "organised crime" *(delitto di criminalità organizzata)* for the applicability of the abovementioned provision: it includes not only the most dangerous mafia (art. 416-*bis* CP) and terrorist criminal organisations (art. 270-*bis* CP), but also the ordinary criminal association (*associazione a delinquere*, art. 416 CPP).[1]

This approach can be criticised as it could lead the prosecutor to abusively use the label of *associazione a delinquere* instead of mere *complicity* (here in the meaning of *concorso di persone nel reato* as ruled by art. 110 CP) in order to use the more convenient interception regime applicable in situations when it does not seem likely that the prosecutor's perspective would be confirmed in the trial.

---

[1] Cassazione penale, sezioni unite, 28-04-2016, n. 26889, Scurato, in CED, rv. 266906.

In the following years, this provision has been referred to by other norms that extend this special and simpler regime of interceptions to many other offences (see below, para. III.B.7.a.) undermining the general regime just described above (para. i).

iii) The recent art. 6 of *decreto legislativo* no. 216 of 29 December 2017 is another example of a special provision prevailing over the ordinary system. For the following reasons, its specificity can be classified as "secondary." This provision allows the use of the interception regime described by the abovementioned art. 13 of *decreto-legge* no. 152 of 13 May 1991 in proceedings concerning crimes committed by public officials against the public administration (such as corruption and *concussione*). The norm is part of the measures adopted in the framework of the fight against corruption, considered as endemic in the field of Italian public administration. The features of art. 6, in particular its subjective and objective limitations (it is applicable only for crimes of public officials against the public administration) and its self-definition as a "derogative regime" (see above, paras i. and ii.), result in the "secondary" nature of its specificity.

The norm can be criticised for different reasons. Not only is its wording misconceived, but the provision introduced an additional case of interceptions, not codified in the Code of Criminal Procedure.

iv) Art. 295(3) CPP, allows telecommunications interception in order to search for suspects at large.

According to the definition provided by art. 296 (1) CPP "an individual at large" is a person who is willingly avoiding or violating personal preventive measures, such as preventive detention *(misura cautelare detentiva)*, house arrest *(arresti domiciliari)*, mandatory residence *(obbligo di residenza)* and travel bans *(divieto di espatrio)*, or violating a detention order, i.e., the executive order for detention after criminal conviction *(ordine di carcerazione)*.

Despite some amendments, art. 295 CPP has been present in the CPP since its approval in 1988, and its applicability is limited and justified by the "at large-status" of the person and the consequent need to search for him.

b) Preventive law

i) On the contrary, preventive interceptions are not connected to crimes that have been committed but are intended to avoid the commission of possible future crimes. They were introduced in the Italian system in the 1970s, against the backdrop of a campaign against subversive terrorism (see art. 226-*sexies* former CPP of

1930) and organised crime (art. 1(8), *decreto-legge* no. 629 of 6 September 1982, enacted by *legge* no. 726 of 12 October 1982).[2]

After the entry into force of the new Code of Criminal Procedure in 1989, the role of preventive interceptions has been limited to art. 266 of the implementation rules of the CPP, the *norme di attuazione, di coordinamento e transitorie del codice di procedura penale (disp. att. CPP)*. In 1992, high profile mafia killings led to the introduction of art. 25-*ter intercettazioni preventive* (i.e., preventive interceptions) in the *decreto-legge* no. 306 of 8 June 1992, enacted with amendments by *legge* no. 356 of 7 August 1992. After the terrorist attacks of 9/11, art. 226 disp. att. CPP was re-written and improved by *decreto-legge* no. 374 of 18 October 2001, enacted with amendments by *legge* no. 438 of 15 December 2001. This new version includes the content of art. 25-*ter* of *decreto-legge* no. 306 del 1992 and was also modified in 2005 and 2015. Today it represents a model for other provisions which refer to its content as examined in para. c) below.

Therefore, according to the current text of art. 226 disp. att. CPP, the Minister of Interior, their delegates and other high officials of police forces can ask the competent public prosecutor for authorisation to intercept communications and conversations "in order to acquire information on prevention" of listed serious crimes. The authorisation lasts for a maximum period of 40 days and the time limit can be repeatedly extended for 20 days. Conveniently, the article states that preventive interceptions cannot be used or even mentioned in criminal proceedings.

ii) Art. 78 *decreto legislativo* no. 159 of 6 September 2011 (the so-called *Codice antimafia*, the "Anti-mafia Act") foresees another type of preventive interception, as it does not assume the previous commission of a crime.

This provision allows the public prosecutor to authorise the police to intercept the communications and conversations of an individual subject to the specific preventive measures provided by art. 6 of *Codice antimafia* (*sorveglianza di pubblica sicurezza*, the *divieto di soggiorno* or the *obbligo di soggiorno*) in order to verify whether the person "is complying with the orders of the prosecutor or is still behaving as he/she did at the time of the issue of the measures." The provision refers to the applicable judicial interception regime provided by art. 268 CPP and the use of the content of preventive interceptions is forbidden in trial.

Art. 78 of the *Codice antimafia* must be read in light of the so-called Italian "preventive measure system" *(sistema delle misure di prevenzione)* as interpreted by the Grand Chamber of the European Court of Human Rights in the case of *De Tommaso v. Italy* (23 February 2017).[3]

---

[2] *Agostini*, Diritto penale contemporaneo, p. 143.

[3] On the topic, see *Basile*, Giurisprudenza italiana, p. 455 ff.; *Basile*, penalecontemporaneo.it., p. 4.

c) Law of intelligence agencies

The so-called intelligence interceptions are a more recent phenomenon than the preventive interceptions governed by art. 226 disp. att. CPP.

As already mentioned, *legge* no. 124 of 3 August 2007 reformed the organisation of the secret services and created the *Sistema di informazione per la sicurezza della Repubblica*. Another relevant provision is art. 4 of *decreto-legge* no. 144 of 27 July 2005, enacted with amendments by *legge* no. 155 of 31 July 2005 and later modified in 2012 and 2015. This norm, covering the prevention of terrorism and subversion activities *(eversione)*, allows the Prime Minister to require the General Prosecutor at the Appeals Court of Rome to authorise preventive interceptions through his powers related to intelligence *(Servizi informativi di Sicurezza)*.

Art. 4 refers to art. 226 disp. att. CPP to determine the basis for interceptions and their use. As preventive interception for the crimes of terrorism and subversion could be authorised pursuant to art. 266 disp. att. CPP, one could doubt the practical utility of art. 4. Nevertheless, it introduces two new aspects as it allows the Prime Minister to request interceptions (while art. 226 disp. att. CPP only mentions the Minister of Interior) and it refers to the General prosecutor at the Appeals Court (instead of the Prosecutor of the Republic at the Tribunal of art. 226 disp. att. CPP).[4]

d) Customs Investigation Service

Customs officials act as both judicial and administrative police in relation to tax law. They work in customs and, upon the delegation of the judicial authority, across the national territory in order to fight against the import, export, and circulation of counterfeited goods.

Within the competence of the Customs Agency *(Agenzia delle Dogane)*, interceptions can also be used to gather information for the judicial authority. However, there are no specific and autonomous provisions ruling interceptions in this particular field.

3. Responsibility for the technical performance of interception measures

As far as the technical aspect of interceptions is concerned, once the judicial, preventive or intelligence interception has been ordered by the judicial authority, it must be implemented.

Police officers act as judicial police in the case of judicial interceptions, or as security police in the case of preventive interceptions or interceptions of intelligence. Naturally, the different kind of interception is irrelevant for the right to secrecy and

[4] *Agostini*, Diritto penale contemporaneo, p. 144.

privacy: any individual has an interest not to be intercepted. If they must be, it must be presumed that they prefer their conversations to be listened to and handled by a few people only, respecting strict procedures and protocols in order to minimise the risk of unlawful listening, leaks and, more generally, unnecessary violations of their fundamental rights.

Looking at the law, the legislator's choice is clear and can be considered a general principle in this field: once an interception is possible, it should be executed by the means available at the *Procura della Repubblica* (the office of the prosecutor with a seat in every local tribunal). The use of external systems, under the supervision of other public or private structures, should be exceptional and always subject to a specific authorisation by the prosecutor (*see* art. 268(3) and (3-*bis*) CPP for judicial interceptions; art. 25-*ter* (2) *decreto-legge* no. 306 of 1992 for preventive interceptions; art. 78(2) *Codice antimafia*, for interceptions related to the adoption of preventive measures, referring to art. 268 CPP).

Looking at the practical and organisational aspects related to judicial interceptions, each Procura della Repubblica has the necessary instruments to intercept telephonic conversations thanks to a dedicated listening room, often known as the centro di intercettazioni telefoniche (CIT). Officials of the judicial police are responsible for its functioning. Once a situation arises where they must intercept, they ask the RTG *(Rete Generale di Telefonia)* or PSTN *(Public Switched Telephone Network)* operators to execute the request coming from the judicial authority through their technological and organisational structures. The designated telecommunications operators divert the phone lines subject to investigations to the CIT of the *Procura della Repubblica* who made the request without the user being aware of the diversion. In this way the intercepted information is available to the judicial authority who, through the designated judicial police, records, listens to, and makes notes of interceptions. These steps have also been recognised in jurisprudence,[5] and distinguished into different phases. The intake phase must be started by the telecommunications operators who divert the communication to the *Procura della Repubblica*. The second phase concerns the recording of the interception and is realised through digital recording systems in centralised IT data storage; all data can then be copied onto digital devices such as DVD, CD, USB, etc. in order to make them available and usable in criminal proceedings. Then comes the listening phase, through which the police is informed of the content of the intercepted conversations that are later verbalised in the last phase: the verbalisation makes the information available for future use.

Many *Procure della Repubblica* have adopted circular letters *(circolari)* in order to create rules on one or many aspects of these delicate phases. The Independent Authority for data protection *(Garante per la protezione dei dati personali)* itself

---

[5] Cassazione penale, sezioni unite, 26-06-2008, n. 36359, Carli, in CED, rv. 240395.

issued an order no. 356/2013 to limit the access to evidence by non-authorised third persons during interceptions, preventing unlawful access or illicit treatment of data. The Authority emphasises the role of CITs, ruling on their logistical functioning and imposing physical and IT security measures, in order to allow access only to officials authorised by the prosecutor and identified by biometric data and to allow access to data by technical personnel, within the limits of their maintenance activities.

Italian law requires recording, listening, and verbalisation activities to be done at seat of the *Procura della Repubblica*, but not necessarily on devices (such as servers) owned by the *Procura* itself. Because of the speed at which IT progresses, the equipment used by the prosecutors is usually rented or hired. It is evident that in these cases particular attention must be drawn to the relationship between the *Procura* and the private owners of the infrastructures, in order to respect the high standard of privacy required by the fundamental right to private life. Another future, yet controversial possibility is the use of *cloud services* to store data.

The above analysis focuses on phone interceptions. There are also more complex interceptions, such as telematic ones or those that can be done by inserting a virus or trojan programme into the computer, tablet or smartphone of the concerned person (the so-called *captatore informatico*). These new interceptions, requiring constantly developing technologies, rely on the know-how of private enterprises. The obligation to respect privacy in data treatment and the rights of the individuals must be granted by all the private subjects involved, in the same terms applicable to the prosecutors.

Concerning preventive interceptions, the scenario is much more unclear, because of security reasons. Due to the fact that there is no reference judge in this process (the majority of preventive interceptions are authorised by the prosecutor upon request of the executive, who uses it for its own purposes), there is no effective control over operations. As a consequence, the *Corte di Cassazione* is prevented from exercising its authoritative power over the process through its jurisprudence.

4. Legitimacy of data transfers between different security agencies

This section will discuss whether interceptions of communications (and in general, acquired data), set up in a specific context can circulate and be used in different destinations.

a) Use of intercepted communications for other purposes

The issue at stake here is the possibility for the content of the interception of communications to be used not only in criminal trials but also in other circumstances by other authorities.

The first problem is whether the results of an interception, authorised in a certain criminal proceeding, can be used in a different criminal proceeding. The law adopts a restrictive approach to grant the rights of the defence of individuals involved in other criminal proceedings. Art. 270 CPP states that the circulation of interceptions is allowed only if "indispensible for the ascertainment" of the serious crimes that allow arrest in the act of committing, listed in art. 380 CPP. In all other cases their use is forbidden.

The second problem is whether the results of an interception, authorised in a criminal proceeding, can be sent to intelligence agencies. The judicial authority and the judicial police have no specific duties in this field, and during the preliminary investigations they are bound by the confidentiality of investigations foreseen by art. 329 CPP. Arts. 118 and 118-*bis* CPP address the opposite situation: the Minister of Interior (art. 118 CPP) and the Prime Minister (art. 118-*bis*) who receive information from "confidential" sources of the existence of a criminal proceeding, have the power to ask the judicial authority to be sent copies of the documents relating to that proceeding despite the confidentiality of investigations, in order to facilitate the prevention of specific crimes. It is a very broad power that entails any act related to criminal proceedings, including interceptions. The judicial authority, which could send the documents to the Minister of Interior and the Prime Minister on its own initiative, can reject the request. If it grants it, the documents remain confidential.

Thirdly, another specific scenario is the interception of conversations of personnel of the secret services *(Servizi di informazione per la sicurezza)*. Art. 270-*bis* CPP balances the need for the prevention of crimes and for the punishment of the perpetrators of those crimes, with the privacy required for the intelligence activities, pursued under the power of the *Presidenza del Consiglio dei Ministri*. Under certain circumstances the *Presidenza del Consiglio dei Ministri* can prevent the use of interceptions by citing the existence of a "state secret." For this reason, arts. 256-*bis* and 256-*ter* CPP, despite not being directly related to the interceptions regime, rule the relationship between the judicial authority and the *Presidenza del Consiglio dei Ministri* when the former needs to acquire "documents, acts or other things" physically detained by intelligence agencies involving the *Presidenza* itself (AISE and AISI detailed above). It must be considered that, if personnel of the secret service are suspected to have committed a crime, they can invoke the application of the special justification/excuse contained in art. 17 of *legge* no. 124 of 3 August 2007.

b) Disclosure of data by intelligence agencies

Another issue at stake, parallel to the one above, is related to the circulation of preventive interceptions. This field is not governed by a clear legal framework.

There is no doubt that the content of these interceptions can be exchanged between different intelligence agencies (both of a civil and military nature), but the

lack of written rules means that their functioning is managed only by opportunity and convenience.

The question relates to whether intelligence agencies have a duty to transfer information or provide updates on their activities to the judicial authority. If preventive interceptions remain bound by their "preventive" function, revealing the possible commission of future planned but not yet committed crimes (and therefore not punishable as attempted crimes), their content should not be of any interest to the judicial authority. Nevertheless, in reality, preventive and investigative activities are closely linked and an interception of a specific conversation can reveal the existence of both committed and planned crimes. Therefore, the intelligence staff members also have a duty to inform the judicial authority about the committed crimes in the same manner as every public official or *incaricati di pubblico servizio on duty* (art. 331 CPP). However, the content of preventive interceptions cannot be used as evidence in criminal proceedings. As stated by the jurisprudence,[6] they could instead be classified as *notizia di reato* (i.e., the information received by the judicial authority or the judicial police related to the possible commission of a crime) or could be used as a legal basis to support a specific investigative activity. In the end, given the state of the art, there are very few instruments in order to assure the compliance with these duties of the intelligence staff.

II. Principles of Telecommunications Interception in Constitutional and Criminal Procedural Law

A. Constitutional Safeguards of Telecommunications

1. Areas of constitutional protection

a) Secrecy of telecommunications

Art. 15 Constitution declares the inviolability of freedom and secrecy of correspondence and of any other form of communication. Such inviolability provides all subjects, including individuals, associations, and organised groups, the right to freely communicate and, as a consequence, the right to send and receive information safeguarding the freedom of expression protected by art. 21 Constitution. The inviolability and secrecy of communications refers to the content of such communications, the identity of the subjects involved and any other information such as data on the time and space of the communication. Moreover, according to the jurisprudence of the *Corte di Cassazione*, the right to privacy is included in the fundamental rights recognised by art. 2 Constitution. For these reasons, the free-

[6] Cassazione penale, sezione II, 19-01-2016, n. 4777, Di Silvio, in *Cassazione penale*, 2016, fasc. 10, p. 3795.

dom and secrecy of communications can be restricted only by acts of the judiciary and within the limits of the guarantees established by law.

The Constitutional Court has interpreted art. 15 Constitution as entailing an absolute rule of law *(riserva di legge assoluta)*. Therefore, only statute law can provide a limitation to this freedom. Furthermore, it is not enough for the judicial decision to be adopted pursuant to a statutory norm, but it also must have adequate motivation, with particular attention paid to the scope, time-limit, and execution of the restriction.

Unlike in the case of *habeas corpus* (art. 13) and inviolability of the home (art. 14), the Italian Constitution does not allow any restrictions to freedom and secrecy of communications by the judicial police, not even in cases of necessity and urgency.

b) Confidentiality and integrity of information systems

In the Italian system, there is no specific constitutional provision regarding privacy and the integrity of information systems. These rights were interpreted in jurisprudence from constitutional norms protecting respectively: freedom and secrecy of communications (art. 15 Constitution), the right to privacy (art. 2 Constitution), freedom of expression (art. 21 Constitution), inviolability of the home (art. 14 Constitution), and the right to private property (art. 42 Constitution).

The privacy and integrity of information systems must be distinguished from the privacy and integrity of data saved and transferred though these systems, as the inviolability of the right to privacy and the freedom of communications implies the protection of the means of communication itself, in order to safeguard the integrity of uploaded and shared data.

c) Right to privacy

As mentioned, the "right to privacy" is not protected by a specific constitutional provision and in the Italian system no clear definition is provided. Nevertheless, the protection of privacy can be derived from traditional constitutional guarantees. This relates to two aspects: the right to data protection as an individual right of the subject to maintain control over their own data; and the right to prevent other people from being informed of their private affairs.

Both of these aspects are grounded in principles protecting the inviolability of the moral freedom of individuals (art. 13 Constitution), inviolability of the home (art. 14 Constitution), and of communications and correspondence (art. 15 Constitution), or declaring the freedom of expression – including the freedom not to express any idea (art. 21 Constitution) – as included among the fundamental rights (art. 2 Constitution).

According to the majority view, the right to privacy is protected in a "static" way and is characterised negatively, i.e., as a right to exclude other individuals from private life. On the contrary, data protection allows a more "dynamic" protection of the personality of the individual and it is an autonomous right since its recent creation. Its conception is rooted in the need for a more intensive protection of the right to privacy because of the increasing use of new cyber technologies.

The right of data protection is the power of each person to control their personal data, or, in other words, the right of the individual to "supervise the circulation of their data." Privacy is at the heart of personality rights and is also a necessary instrument for the development of social life.

According to art. 2 Constitution, the right to privacy is the engine for the realisation of human personality and it is an inviolable right whose content cannot be modified even by amending the Constitution: therefore, a high standard of protection must be granted. At the same time, arts. 15 ff. Constitution state that this right cannot be subject to any limitation, unless the restriction is required by the need to safeguard another primary interest recognised and protected by the Constitution.

The need to prevent and repress crimes, as a necessary requirement for the rule of law (here meaning *stato di diritto*), can challenge the right to privacy of individuals. When balancing the contrasting values, the right to privacy takes a secondary role, but only if and where the restriction is indispensable for the protection of the other value and in light of the principle of proportionality.

It is important to note that privacy and data protection are enshrined in two important international law sources: firstly art. 8 European Convention on Human Rights (ECHR), which recognises the respect for private and family life, home. and correspondence. The second one is European Union Charter of Fundamental Rights (EUCFR), and in particular arts. 7 and 8. Both of these sources have primacy in the Italian legal order.

These national and international principles are implemented by the provisions of the Code of Criminal Procedure, *decreto legislavito* no. 196 of 30 June 2003 (the so-called Privacy Code) and other special norms and executive orders.

d) Right to informational self-determination

The right to informational self-determination is one of the typical new generation rights, a consequence of the development of the Internet and digital technologies. It is therefore quite understandable that the Constitution does not include any provisions on this topic.

The only (soft law) instrument to mention it is the "Declaration on the Rights of Internet" *(Dichiarazione dei diritti in Internet)*, adopted on 28 July 2015 by the "Commission for rights and duties in Internet" of one of the Houses of the Parlia-

ment *(Commissione per i diritti e i doveri in internet della Camera dei Deputati)*. Art. 6 of the Declaration is entirely dedicated to informational self-determination. A person has the right to access their own data, and ask for its integration, amendment and cancellation pursuant to the law, irrespective of the subject holding it and of the place where it is stored. It states that "each individual has the right to know how data related to his/her personality are treated" and that "data collecting and retention must be implemented for the strictly necessary time, respecting the scope and the principle of proportionality ad the right to self-determination of the individuals involved."

Following this definition, the right seems to be protected, even if not expressly, by many provisions of *decreto legislativo* n. 196 of 30 June 2003 and by related case law; and, at the constitutional level, by the abovementioned provisions, i.e., arts. 2 and 15 Constitution, art. 8 ECHR and arts. 7 and 8 EUCFR.

2. Proportionality of access to data

In comparison with other legal systems, for example in Germany, the role of the proportionality principle in criminal proceedings has only recently drawn the attention of academics, jurisprudence and of the legislator. Since the Constitution does not expressly declare the existence of this principle,[7] most of the input comes from the European Union and the ECHR.

As far as criminal procedure law is concerned, the proportionality principle is well known in a very specific framework, i.e., in the context of the personal preventive measures (art. 275 CPP): preventive measures applied to the accused must be proportionate to the alleged facts and to the sanction reasonably applicable at the end of the trial. Only the respect of the proportionality principle can assure the absence of unnecessary restrictions to the defendant's personal freedom, which could be unjustified in respect of the values (often social security) protected through these restrictions.[8]

The ECHR framework is different. Art. 8 includes a proportionality clause, which states:

> (…) the right to respect for private and family life can be limited by a public authority only in accordance with the law and only when it is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The European Union system has recognised the principle of proportionality for a long time, intended as the obligation for public powers to minimise any interfer-

---

[7] The scrutiny of the Constitutional Court according to art. 3 Constitution (principle of equality) is completely different.

[8] See *Tabasco*, Principio di proporzionalità e misure cautelari, Cedam, Padova 2017.

ence in fundamental rights recognised to citizens. Regardless of the fact that the principle of subsidiarity in EU law could also be considered part of the proportionality principle, the latter is expressly affirmed in art. 52 para. 1 European Union Charta of Fundamental Rights ("Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.")

As far as criminal procedural law is concerned, the recent Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014, regarding the European Investigation Order in criminal matters (EIO) acknowledged the proportionality principle: art. 6 para. 1 lit. a) ("The issuing authority may only issue an EIO where the following conditions have been met: (a) the issuing of the EIO is necessary and proportionate for the purpose of the proceedings referred to in Article 4 taking into account the rights of the suspected or accused person") and art. 10 para. 3 ("The executing authority may also have recourse to an investigative measure other than that indicated in the EIO where the investigative measure selected by the executing authority would achieve the same result by less intrusive means the principle of proportionality, even if not than the investigative measure indicated in the EIO") are particularly significant. The abovementioned directive was transposed into Italian law with the *decreto legislativo* n. 108 of 21 June 2017. Art. 7 of the decree ("The investigation order is not proportionate if its execution causes a sacrifice to the rights and liberties of the accused or the person under investigation or other individuals involved in the implementation of the requested acts, not justified by investigative and evidence needs in the concrete case, in light of the seriousness of the offences and the foreseen sanctions") and art. 9 para. 2 ("In agreement with the emission authority, execution is implemented through one or more different acts, appropriate to the same scope, if the investigation order itself is disproportionate, according to art. 7") expressly require the EIO to be respectful. Therefore, this principle is now part of national law, but it is not clear how it will develop.

In the ordinary (sub-constitutional) interception regime, proportionality is not expressly recognised.

a) Implications for invasions of the secrecy of telecommunications

As mentioned above, the ordinary regime for telecommunications interceptions (art. 266 ff. CPP) does not specifically recognise the proportionality principle. Nevertheless, the regime is consistent with the principle. Statutory law allows interceptions in only a few specific situations, and provides a precise and accurate

procedure. Ultimately, and above all, it implies its "inadmissibility" *(inutilizzabilità)* in case of a violation of the foreseen procedures.

In conclusion, the principle of proportionality, even if not expressly *stated* in the ordinary regime for interceptions, is *implemented* in practice.

b) Implications for access to traffic data

Data retention is ruled by art. 132 of the so-called Privacy Code and by other special norms, such as art. 24 of *legge* no. 167 of 20 November 2017 (also known as *legge europea 2017*).

These provisions seem to violate the principle of proportionality as they allow for data retention with respect to every kind of offence, and in certain cases they recognise the right of the judiciary to have access to data for 72 months. It means that communications service providers have the obligation to hold data for a very long time.

The subsequent sacrifice of the privacy of citizens' personal data is clearly disproportionate and an intervention by the legislator in this matter is desirable.

c) Implications for intrusion into information systems

The framework of the intrusion in IT systems is a complex issue. If intrusion into IT systems is defined as an intrusion that takes place without data owners, system administrators, and other people involved becoming aware of this intrusion, then it must be recognised that this type of investigative act is not regulated in Italy. Even allowing investigative activities outside the legal framework, the problem of the proportionality principle is still at stake: in the absence of any legal basis governing the cases and execution of intrusions, the principle in question will never be respected. The related problems will be analysed in the following paragraphs.

3. Consequences for the interception of telecommunications

If Italian law only proclaimed the inviolability of a certain right without providing for the consequences of the violations, the guarantees for citizens would remain mere declarations and empty petitions of principle which would be unacceptable. Criminal law offers two potential different reactions in the case of fundamental rights violations: it can develop a provision describing a criminal offence for the perpetrator of the violation (substantive criminal law reaction); or it can foresee a procedural sanction for the acts committed in violation of the right during a criminal trial (criminal procedural law reaction). The first kind of reaction will be analysed in para. 4(a) and the latter will be taken into consideration in the next paragraph.

a) Protection of the secrecy of telecommunications

Communications interceptions that violate the norms of the Code of Criminal Procedure (arts. 266 ff. CPP) are sanctioned with inadmissibility *(inutilizzabilità)* (art. 271 CPP), which can be raised in every phase of the proceeding (art. 191 para. 2 CPP). In this way, the system deters the practice of intercepting communications outside the foreseen cases or without compliance with the formalities imposed.

b) Protection of the confidentiality and integrity of information systems

As mentioned above (see para. 2.c.), there are no provisions prescribing the power, for the judiciary or the police, to secretly intrude on IT systems for investigative purposes.

As a consequence, the law itself does not provide for specific sanctions, unless we consider every unauthorised investigation act affecting fundamental rights (as it should be) forbidden as such, and therefore inadmissible (technically *inutilizzabili*, i.e., not usable) in trial.

c) Protection of the core area of privacy

The core area of privacy is protected by the abovementioned constitutional and supranational norms and is specifically recognised in ordinary law, particularly in the Privacy Code (*decreto legislativo* no. 196 of 30 June 2003).

The Privacy Code is a complex normative act, which, in addition to norms of principle, details the way in which citizens' personal data must be protected. Different data categories (i.e., sensitive data, judicial data, etc.) are taken into consideration and governed by different provisions.

A norm of principle, art. 11(2) states: "Personal data handled in violation of the relevant data protection discipline cannot be used." It could be argued that, because of this provision, personal data *handled* in violation of the Privacy Code, as in violation of any other relevant provision, cannot be used on any occasion, not even in a criminal proceeding. In reality, Italian jurisprudence has always refused such an approach and art. 11(2) Privacy Code remains merely a declaratory provision.

Therefore, not all violations of the privacy regime are adequately protected in criminal proceedings and the approach can change on a case to case basis. For example, thanks to an amendment of 2009 (*legge* no. 85 of 30 June 2009), the legislator provided a quite organic regime for the possibility to draw and use genetic samples in criminal trials with adequate illustrations of hypothesis, techniques, and sanctions (arts. 224 *bis* and 359 *bis* CPP).

4. Statutory protection of personal data

a) Criminal liability for the unlawful infringement of telecommunications

Illegitimate violations of the secrecy and privacy of communications can trigger the applicability of provisions of criminal law, and the discipline is stricter when the person responsible is a public official (see below para. III.B.1.c.).

b) Protection of professional secrets in criminal procedural law

Secrecy is clearly a limitation to fact finding in criminal cases.

The notion of the 'professional secret' is quite problematic as it is difficult to identify individuals who can raise its existence and refuse to provide information to the judiciary and the investigators (art. 200 CPP mentions, for example, clergymen, lawyers, and journalists). The code also contains a provision on official secrecy in art. 201 CPP and state secrets in art. 202 CPP.

Distinguishing between different secrets, procedural provisions identify whether and possibly how the need for fact finding can prevail (see below, III.B.3.aa.).

c) Principle of "purpose limitation of personal data"

The principle of "purpose limitation of personal data" determines that, when personal data is collected – with or without the consent of the holder – by a certain authority and with a certain purpose, data cannot be transferred to any other authority and/or used for a different purpose. More specifically, the purpose limitation principle consists of two elements: first of all data must be collected for specified, explicit, and legitimate purposes only (purpose specification); secondly, data must not be further processed in a way that is incompatible with those purposes (compatible use).

As this principle is part of EU law, it must be incorporated into the national legal orders of the Member States. This is true for Italy: art. 11(1)(b) Privacy Code states that personal data is "collected and stored with specific explicit and legitimate purposes, and it is used in other operations in a way that is compatible with these purposes:" it is therefore clear that any use that is incompatible with the purpose at the origin of the collection of data is forbidden.

The mandatory nature of this provision and its effect in criminal trials is a matter for debate. The purpose limitation principle is not mentioned by any procedural provision, nor is any duty to destroy or cancel data when it is no longer necessary for the criminal trial.

The matter seems to fall outside the framework of the criminal trial, and it seems to be attributable to the general theme of the right to oblivion: this right includes

the power of the owner of the data to ask for the cancellation, pseudonymisation or anonymisation of their data.

B. Powers in the Code of Criminal Procedure

1. Requirement of (reasonable) clarity for powers in the law of criminal procedure

The principle of *nullum crimen sine lege* is a cornerstone of the system at both a national (art. 25(2) Constitution) and supranational level (art. 7 ECHR and art. 49 EUCFR).

An important question is whether an analogous qualitative standard should be extended for criminal procedural provisions. It is clear that substantive and procedural provisions must be distinguished and the existence of a gap between these two "worlds" has been recently highlighted in the *Taricco* decisions, where the Italian Constitutional Court and the Court of Justice of the European Union (CJEU) adopted opposite positions while debating, amongst other things, the nature of the statute of limitations' provisions. The matter was solved by the Constitutional Court in its judgment no. 115 of 2018.[9]

Despite the undeniable difference, procedural provisions must clarify in which cases and in which way they limit personal freedoms, especially when they impose a limitation of a fundamental right (for example, the right to privacy). It means that they must respect a certain standard of clarity and precision in order to give people the possibility to know and foresee *ex ante* the possible intrusion of public powers on the enjoyment of their fundamental rights.

There are two ways to reach this result:

– through art. 111(1) Constitution, introduced in 1999, stating that the jurisdiction is implemented through the principle of fair trial "ruled by the law" (and therefore the law must rule its features). This provision, according to certain doctrine, gives specific form to the principle of legality in procedural law as corollary of the principle of legality in substantive law;[10] or
– through enhancing constitutional provisions declaring the inviolability of specific fundamental rights such as *habeas corpus*, inviolability of the home, secrecy of communications, and privacy. All these rights, affected by investigative acts, are protected by the principle of legality and the rule of law (herein "riserva di legge"). It is obvious that the law must be clear and precise in detailing the powers of intrusion given to the public authority.

---

[9] Among others, see *Cupelli*, Diritto penale contemporaneo, pp. 227 ff.

[10] Cfr. *Marcolini/Militello/Ruggieri*, in Bernardi/Cupelli (eds.), *Il caso Taricco e il dialogo tra le Corti*, Jovene, Napoli 2017, pp. 223 ff.

This opinion does not find unanimous support among scholars. Nevertheless, the need to outline in a clear manner the boundaries of the public powers in carrying out investigative measure is widely understood.

2. Differentiation and classification of powers in the law of criminal procedure

In criminal proceedings, the judicial authority and the police are provided with different investigative tools, whose application can be calibrated according to the different type of offences, and in light of their seriousness, or to the different evidence needs. The use of these means is governed by reason and, as a secondary consideration, by proportionality.

A classic example is that of the public powers searching for a precise object in the domicile of an individual. Before starting the search in the individual's house, the police will ask the person to hand over the object. If the person spontaneously completes the request, the search (a more thorough and intrusive act) does not take place, with satisfaction to both sides (art. 248 CPP).

Therefore, as in many modern legal systems, the Italian legislator discretionally rules on investigations in order to balance the pursuit of truth with the protection of personal freedom on a case to case basis (the greater the sacrifice, the more prudent the use of the investigation tool must be).

If one was to imagine a new procedural system, the approach of the "Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office" (COM/2013/0534 final), transposing the "Model Rules" elaborated by the University of Luxembourg in an EU-financed study, is a highly attractive model. Art. 26 of the Proposal, "Investigating measures," details a strict list of investigation acts (para. 1); it contains an expressed proportionality principle (para. 3: "the individual investigative measures referred to in paragraph 1 shall not be ordered without reasonable grounds and if less intrusive means can achieve the same objective"); furthermore, it divides investigative acts according to their intrusive effect, distinguishing between acts that the European Public Prosecutor's Office can implement discretionally, and acts that must be authorised by a judge.[11]

The question to be answered is the following. In paragraph 1 we analysed how substantial and procedural criminal law should be clear and precise in regulating investigation activities if they intrude upon a citizen's freedom. Nowadays, technological progress allows investigators to investigate in new ways, but the legislator is not always able to translate this into codified investigative rules. For example, the so-called satellite surveillance, which is executed by hiding a GPS under the

[11] The project of the Commission was only partially followed in the drafting of EPPO Regulation no. 2017/1939.

person under investigation's car to monitor their movements remotely, is not regulated by any provision in Italian law.[12]

The question here is whether an act of this character:

– can be considered as evidence, i.e., whether it increases the knowledge of investigators;
– violates fundamental rights of the individual (not only the person under investigation, but also of other persons close to them);
– is not prescribed by law;
– can be executed by public powers.

The traditional Italian approach would affirm the principle of the "atypical nature" of investigations: the investigator can implement every act useful for the finding of the truth, even if they are not prescribed by law.

This is a rather old-fashioned approach. A more modern approach would state that if these acts impose a restriction of fundamental rights protected by the principle of legality and the rule of law, a statutory basis for the action is essential.[13]

III. Powers for Accessing Telecommunications Data in the Law of Criminal Procedure

A. Overview

As far as interception of communications in a criminal trial is concerned, the following provisions and possibilities must be taken into consideration:

– arts. 266 ff. CPP, governing the interception of the content of communications. Usually scholars distinguish between telephonic communications (between people over a distance) and in-person communications, when the people involved are all in the same place (in order to intercept them it is therefore necessary to resort to the so-called "intercettazioni ambientali," i.e., audio surveillance);
– art. 266-*bis* CPP, in particular, extending wiretapping to cyber- and telematic communications;
– art. 13 of *decreto-legge* no. 152 of 13 May 1991, signed into law with amendments by *legge n*o. 203 of 12 July 1991 (for associate crimes) and art. 6 of *decreto legislativo* no. 216 of 29 December 2017 (for crimes committed by public officials against the public administration);

---

[12] The example is interesting because it is the subject of the European Court of Human Rights' judgment of 2 September 2010, *Uzun v. Germany* (ric. n. 35623/05).

[13] See Marcolini, *Cassazione penale*, 2015, vol. 2, pp. 760 ff.

– art. 247 paragraph 1-*bis* CPP, stating that if the communications have already taken place (for example, the email has already been sent and received by the addressee) it is possible to use a "cyber search" of the system where the communication has been filed. The search can never be secret, as it always requires the exhibition of a judicial authorisation. The discovered communications can naturally be seized according to arts. 253 ff. CPP;
– art. 132 Privacy Code when it is necessary to collect the external traffic data, not the content of the communication (so-called data retention).

B. Interception of Content Data

1. Statutory provisions

The fundamental regime for the interception of communications is provided by arts. 266 ff. CPP.

Art. 266 CPP enumerates the crimes that justify a request for authorisation of interception. There are two main leading criteria: one quantitative and one qualitative. According to the quantitative criterion, interceptions are allowed in relation to "culpable offences punished with life sentence or imprisonment of more than five years in maximum." The qualitative criterion allows interceptions for a series of crimes enumerated in para. 1 letter b) and ff., such as drugs crimes and weapons smuggling, but also less grave crimes such as "molestia o disturbo delle persone" (art. 660 CP) committed by telephone.

Art. 267 CPP is important as it states that interceptions are allowed only if supported by "serious evidence of crimes" *(gravi indizi di reato)* and only if "absolutely indispensible for the prosecution of the investigations." Moreover, it identifies the legitimate subjects in the completion of the act: the prosecutor presents the request to the pre-trial judge *(giudice per le indagini preliminari)*. Once the prosecutor is authorised, they oversee the operations that last for 15 days, extendable for another 15 days (there is no limit to the number of extensions).

Arts. 268–269 CPP govern the execution of the operations, usually entrusted by the prosecutor to the judicial police, and the delicate phase of recording and transcription of the contents.

Art. 270 CPP describes under which circumstances the interceptions made in a specific criminal proceeding can be used in a different one.

Finally, art. 271 CPP promulgates the sanctions. It states that interceptions are inadmissible *(inutilizzabili)* if carried out outside the law or in violation of the main procedural norms. This provision is of primary importance as it would be a nonsense to declare the inviolability of a certain fundamental right (in this case the secrecy of communications) if the public authority could violate its limits without

any consequence. For many years after the entry into force of the Code of Criminal Procedure in 1989, all the abovementioned articles (266–71 CPP) were subject to many exceptions and issues, coming from the defence of the persons accused in criminal trials, and the case law of the *Corte di Cassazione* in plenary session has helped to interpret them coherently.

2. Scope of application

a) Object of interception

According to art. 266 CPP, the possible objects of interceptions are "conversations," "telephonic communications," and "other forms of telecommunications." According to art. 266-*bis* CPP it is also possible to intercept the "flow of communications related to cyber- and telematic systems, or between different systems" *(flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi)*. Procedural law does not provide a definition of these expressions.

aa) Content of communications

The content of communications can be varied (an order, a piece of information, a message, a code-message, etc.), but it must be a communication, i.e., it must involve the transmission of a thought relevant to the investigations.

In general, communications can possess any form: not only verbal communications, but also written or gestural ones.[14] Sign language is a good example of communication by gesture. The communication can also consist of "communicative behaviours" *(comportamenti comunicativi)*, i.e., behaviours which aim to transmit the content of thoughts through words, gestures, face reading expression or other attitudes.[15] The distinction between communicative and non-communicative behaviours has for long time been a prolific subject in debate among scholars: it has been noted, for example, that if a private citizen video-records two persons communicating through communicative behaviours, they are illegally intercepting communications and the illegality comes from the private nature of the agent. The recording is therefore inadmissible in trial. On the contrary, if that very same agent video-records two persons doing something without communicating, it is possible to admit the film as evidence in trial (as documentary or atypical evidence).

---

[14] Cassazione penale, sezione V, 20-09-2017, n. 53181, in Banca Dati DeJure.

[15] Cassazione penale, sezione III, 23-11-2017, n. 4744, in Banca Dati DeJure.

bb) Communication between persons

Usually the communication involves at least two persons and an exchange of thoughts between them. There is no doubt that many provisions of the CPP assume this form of communication. Nevertheless, the advancement of information technology clearly demonstrates that the law should also consider other new situations.

Without evoking futuristic scenarios where AI systems can dialogue with human beings or other systems, communication between a person and an automated information system (such as a communication with a webserver while downloading a file from a website), or the traffic between computers and data storage in cloud servers or other remote storage or data processing systems, or the traffic between two independent computer systems (for example, between a computer and a server for planned update- or backup-operations) is already possible.

Given that the jurisprudence has not consciously faced this problem yet and leaving aside the technical problems linked to interceptions of communication through systems, art. 266-*bis* CPP allows interceptions of the "flow of communications related to cyber- and telematic systems, or between different systems." This expression is wide enough to include the abovementioned examples.

Nevertheless, it is probably better to limit the applicability of the investigative act of "interception of communications" to communications between persons, rather than systems, in light of the strict interpretation of provisions involving intrusions into the fundamental rights of the citizens.

Naturally, the legislator has the power to submit all types of interceptions to the same regime, for example, by providing that "the expression interception of communications includes also communications between a person and a system or between systems." Another alternative is to create an *ad hoc* investigative measure, entirely dedicated to intercepting communications between persons and systems.

cc) Surfing as telecommunication

The main problems in this area have already been mentioned in the previous paragraph. Surfing on the web includes an exchange of data between the surfing device and the visited web-sites. Despite this exchange, there is no communication and the person can even be unaware of this data exchange. Therefore, mere "surfing on the web" should not be qualified as "telecommunication."

However, it does not mean that this information is of no interest for the judicial authority and the police, but interception is not the instrument to be used during investigations in order to obtain it. The jurisprudence still has to clarify these aspects.

b) Temporal limits of telecommunications

aa) Access to ongoing telecommunications

In Italy, interceptions are allowed only during and because of the transmission of communicative data. Therefore, they are intrinsically "dynamic," as without transmission of data no interception is possible.

bb) Access after the end of telecommunication transmission

In order to obtain access to data before or after its communication, it is necessary to use other instruments, in particular information searches (art. 247 CPP) and the seizure of data (arts. 253 ff. CPP).

The negative aspect of these activities is that they are not secret. In Italy, there is no legal instrument to conduct an online search or online surveillance without the person being aware of it.

c) Current matters of dispute

aa) "Source telecommunication surveillance"

The expression "source telecommunication surveillance" is linked to an episode that occurred in the German Federal Republic when government agencies produced, and used in criminal investigations, the so-called government malware or "Staatstrojaner." A national malware can be programmed in order to infiltrate a device and can carry out a high number of activities; the activity of the malware considered here should be limited to the interception of communications on the device directly from the source ("source telecommunication surveillance") without asking telephonic or telecommunications service providers to intercede.

From a technical perspective, this system is surely valid, and it has many advantages. Nevertheless, at the same time it raises important problems. The main issue is that there is no assurance that a national malware limits its activities to the interception of communications and does not also collect other data available on the device.

In Italy, similar software could fit into the interception regime only as far as it allows the interception of communications made through and received by a device.

For some issues see below para. dd.

bb) Access to external storage media as communication

Since cloud computing and external storage media are widespread phenomena, it is important to establish whether data exchange between the terminal of the service

holder and its partition in the cloud should be considered a form of communication and therefore open to possible interception. This question can also be raised in relation to the upload and download of data, as the synchronisation includes them both.

In light of what has been discussed in the previous paragraphs, this kind of exchange should not be considered "communications" as it is not an exchange between persons who intend to communicate each other. Therefore, the interception regime should not be applied.

There is no relevant jurisprudence on this issue though.

cc) Evaluation of surfing behaviour

The behaviour of a person on the web – considering both the sites they visit and the words they input into a search engine – can reveal many aspects of their personality and habits. It has not been demonstrated that visits to public sites are confidential. Two problems must be faced:

– the first is linked to substantive criminal law: does compiling a profile of a person on the basis of their surfing habits have any relevance in criminal research? Or is there the risk of (unacceptably) transforming "factual-based criminal law" into "author-based criminal law"?
– the second problem is connected to procedural law: once again, it must be highlighted that – even in the absence of precise jurisprudence on this issue – people surfing on the Internet are not communicating and, therefore, cannot be intercepted according to arts. 266 ff. CPP.

dd) The Italian "captatore informatico"

A special mention should be given to the Italian "captatore informatico" as it makes it possible to better comprehend the conclusions of other current matters of dispute.

In Italy, the German "Staatstrojaner" was called "virus o Trojan di Stato" until it was legally renamed "captatore informatico" by the legislator in 2017.

First of all, it is appropriate to quote the words of the Corte di Cassazione in plenary session explaining the high potential of this instrument:

> "Before addressing the juridical problems, it is better to highlight the main technical and cyber features of this investigative instrument.
>
> Interceptions are made through a software, usually a Trojan horse, called "captatore informatico" (sez. 5, n. 16556 of 14/10/2009, Virruso, rv. 246954) or "agente intrusore" (sez. 6, n. 27100 of 26/05/2015, Musumeci, rv. 265654).
>
> The program is installed on a target-device (a computer, a tablet or a smartphone), usually from a remote location and secretly, through an e-mail, a text or an adjourning application. The software is made of two parts: the first one (server) is a small program in-

fecting the target-device; the second one (client) is the application used by the virus to control the device.

Such an instrument allows many activities, in particular:

to detect the data traffic from and to the infected device (surfing and e-mail, both web-mail and outlook);

to activate the microphone and therefore catch conversations in the area surrounding the holder of the device, wherever he/she is;

to activate the webcam, allowing the capture of images;

to search the hard disk and copy entirely or partially the memory units of the cyber-system under attack;

to decode whatever is typed on the keyboard (keylogger) and catch what appears on the screen of the target device (screenshot);

to circumvent normal antivirus software.

The data collected in this way is transmitted over the Internet in real time or on a regular basis to another cyber-system used by investigators.

It is easy to imagine that this will be very useful during investigations and will open up new possibilities.

Nowadays, long-distance communication is usually done through cyber instruments, as it is cheaper and has more potential than the telephonic line.

Using the abovementioned program – infecting a mobile phone, a tablet, a PC – it is also possible to catch conversations between people talking in the same place, and in these cases the interception becomes an "ambientale" interception [audio surveillance]. Mobile phones, tablets and notebooks are part of everyday life and follow their owners, therefore using them for interceptions makes it possible to control the person's life. This surveillance necessarily interferes in the sphere of people living close to the intercepted person.

This kind of audio surveillance can be done everywhere, therefore also inside a private house and not only in public places, and investigators can circumvent the problems connected to the installation of wires, reducing the risk of discovery.

Therefore, this instrument imposes an assessment in balancing the investigative exigencies, that suggest it will be used recurrently and its potential is yet to be fully discovered, and the need to respect individual rights, that can be seriously harmed. Some scholars have stated that "the fundamental rights are subject to a "progressive protection" not only because their protection must follow the evolution of the technology and the test of time, but also because they face the exigency – imposed itself by the Constitution – to prosecute crimes." [16]

For its extreme utility, the *captatore informatico* was used in criminal investigations before 2017, when the legislator decided to create an autonomous regime: the abovementioned extract of the judgment of 2016 is a clear demonstration of this as it also cites previous judgments.

Art. 1 para. 84, letter e), no. from 1) to 8) of the *legge* no. 103 of 23 June 2017 (known as "Legge Orlando" from the name of the Minister of Justice of that time) gave the Government the authorisation to issue a *decreto legislativo* with the aim of

[16] Cassazione penale, sezioni unite, 28-04-2016, n. 26889, Scurato, Considerato in Diritto, paragrafo 2, in Banca Dati De Jure.

establishing the use of the *captatore informatico* in criminal proceedings, but only for audio surveillance (see the *chapeau* of para. 84).

The Government issued the *decreto legislativo* no. 216 of 29 December 2017. This decree also partially modified the interceptions regime, but important for this study is the new regulation of the *captatore informatico*:

– art. 4 concerns the amendments to the CP;
– art. 5 concerns the amendments to the *disposizioni di attuazione* of the CP;
– art. 7 contains the implementing rules;
– art. 9 contains the transitional regime, i.e., the regime applicable at the entry into force of the decree.

It is worth reaffirming the clear choice made by the legislator in 2017: the *captatore informatico* is applicable only for audio surveillance. Nevertheless, it is self-evident that this is only one of its possible uses.

Thus, art. 4 of the *decreto legislativo* no. 2016 of 2017:

– modifies art. 266 para. 2 CPP, now stating that: "in the same cases[17] audio surveillance is allowed *also through the installation of a captatore informatico on an electronic device*. Nevertheless, when communications take place in the places listed in art. 614 CP, interception is allowed only if there are reasonable grounds to believe that a criminal activity is ongoing in that place" (emphasis added);
– introduces art. 266 para. 2-*bis* CPP, stating that "audio surveillance through the captatore informatico on an electronic device is always allowed in the proceedings for the crimes listed in art. 51, paras 3-*bis* and 3-*quater*" CPP (i.e., organised crimes and terrorism). Therefore, for these types of crimes the use of the captatore informatico is – comprehensively – facilitated;
– modifies art. 267 CPP, imposing on the judge authorising the use of the *captatore* (and the prosecutor in case of urgency) the duty to support their decision and reason the choice of this tool. Moreover, in cases of organised crime and terrorism, the judge must indicate the place and time when it is possible to switch the microphone on;
– introduces art. 270, para 1-*bis* CPP extending the use of interceptions through the *captatore* to other new crimes;
– introduces art. 271 para. 1-*bis* CPP, sanctioning with inadmissibility *(inutilizzabilità)* the collection of data through the *captatore* beyond the limits of time and place of the authorisation.

Some other provisions of the *decreto legislativo* no. 216 of 2017 are of special relevance:

---

[17] The provision refers to the previous paragraph, ruling wiretapping.

Art. 5 amends art. 89 disp. att. CPP. The new para. 2-*bis* states that "only programs respecting technical parameters identified by the Minister of Justice by decree can be installed on electronic devices for interceptions."

Art. 7 is linked to the explanations detailed in the previous paragraph, as it states that "the technical requirements of the cyber-programs for interceptions through the *captatore informatico* on an electronic device are decided with decree of the Minister of Justice to be issued within thirty days from the entry into force of this decree."[18] The technical provisions are therefore very important also for lawyers as spy programs must respect the strict (updatable) ministerial standards.

Art. 9 provided that the *captatore* could be used for interceptions only 180 days after the entry into force of the decree, on 26 July 2018, but the Government issued the *decreto-legge* no. 91 of 25 July 2018 (enacted with amendments by *legge* no. 108 of 21 September 2018), whose art. 2 postpones the starting date until "after 31 March 2019."

Journalistic sources suggest that the postponement of the entry into force of the *captatore informatico*'s regime to after 31 March 2019 provides the opportunity for the majority to intervene – hopefully in an organic and non-selective way – in the area of interceptions.

Until then, the outstanding problem for the *captatore informatico* is the following: as malware has great technical potential, does it make sense to limit its use only to audio surveillance? If the legislator limits the regime of the *captatore informatico* only to audio surveillance, what about the other possible uses (for example, switching the camera on, copying the memory of the device, getting passwords, etc.)? Are they allowed?

These topics are still discussed among scholars and as yet there is no jurisprudence.[19]

3. Special protection of confidential communications

a) Privileged communications

aa) Professional secrets

The regime governing secrets, as a possible limitation to interceptions, is organised in the Italian system as follows.

---

[18] "This decree" is *decreto legislativo* no. 216 of 2017 published on the Gazzetta Ufficiale on 11 January 2018 and entered into force on 26 January 2018. The time limit to issue the second decree with the technical requisites was therefore 26 February 2018.

[19] On the *captatore informatico*, see Torre M., Giuffrè, Milano 2017. On the reform of interceptions see Vv. Aa. Bene T., Cacucci (eds.), Bari 2018.

First, the criminal trial distinguishes between three kinds of special protection of secrecy for the purpose of the interception of communications:

– the so-called professional secret *(segreto professionale)* is ruled by art. 200 CPP. Without imposing any duty, the provision recognises the possibility for a person not to testify on certain known facts because of their functions as clergymen, lawyers, healthcare professionals, and, according to the open clause of para. 1, letter d), to all those with functions the law recognises as permitting to refrain from testifying on issues covered by professional secrecy (such as the operators working in community services for drug dependence: see art. 120 para. 7 of the *Decreto del Presidente della Repubblica* no. 309 of 1990). The secrecy for journalists is much more limited, as it includes only the names of their sources and the judge can force them to reveal such names when it is necessary for the ascertainment of facts (para. 3);
– the so-called official secrecy *(segreto d'ufficio)* is ruled by art. 201 CPP. It provides the duty (not a mere power) for public officials not to testify on facts which must remain secret because of their professional functions. In order to understand official secrecy, it is helpful to refer to art. 326 CP, sanctioning the violation of official secrecy. For example, the secret of the *camera di consiglio* prevents judges from making public the discussions and the votes leading to a decision (art. 125 para. 4 CPP): a judge should never reveal the position or the opinion of a colleague. So doing is an offence sanctioned by art. 685 CP;
– the national secret *(segreto di stato)*, governed by art. 202 CPP, again limiting public officials. The discipline is governed in detail by *legge* no. 124 of 3 August 2017 and subsequent amendments.

The relatives (literally *prossimi congiunti*, the definition of which is provided for by art. 307 para. 4 CP) of an accused cannot oppose the existence of a secret in trial, but art. 199 CPP gives them the power of abstention: when they are requested to make statements, the judge or the prosecutor must inform them that they can decide not to testify. This power is precluded if the relative is suing the accused or is the victim of the offence.

Coming back to the secrets' regime, the object of the abovementioned provisions is to prevent a declaration from being made during the testimony in trial, but it is self-evident that a secret could be violated also in other circumstances before the beginning of the trial or the starting of the testimony.

First of all, if the secret information is contained in a document, it could be the object of a search or a seizure. In this way it would be easy to bypass the abovementioned provisions. Therefore, art. 256 CPP for both professional secrets and official secrecy, and arts. 256-*bis* and 256-*ter* CPP for national secrets, grant the same protection to documents.

In the second instance, secret information can be the object of an interception of communication between persons. Art. 271 para. 2 CPP states that interceptions of

communications protected by professional secrecy are inadmissible *(inutilizzabili)* when they focus on facts known because of the functions, office or profession, unless the persons have already testified on these facts or made them public in any other way (see below para. III.B.9.b.). As far as defence counsels are concerned, the level of protection is stronger as it is assured by art. 103 para. 5 CPP that: "the interception of conversations or communications between defence counsels, private investigators, experts, and their assistants, or between these categories and the people they defend or assist is not allowed." As far as national secrets are concerned, the relevant provision is art. 270 CPP. Finally, despite its unclear location in the code, art. 240, paras. 2–6 govern the destruction of illegal interceptions. This general provision was introduced in 2006. For a detailed analysis of this provision see below para. III.B.9.b.).

Members of Parliament are in a peculiar position, as art. 68 para. 3 Constitution states that each House (*Camera dei Deputati* and *Senato della Repubblica*) must authorise any interception of conversations and communications and the seizure of correspondence. Art. 3 of *legge* no. 140 of 20 June 2003 grants protection also against indirect interceptions, i.e., when the communication of a parliamentarian is intercepted because they are communicating with an intercepted person, but the parliamentarian is not the target of the interception. The problem is to balance the parliamentarian's prerogatives with the legitimate interest in preventing the commission of crimes perpetrated by the originally intercepted person. Analogous protection is granted to other Constitutional organs (see below, para. III.B.6.a.).

b) Responsibility for ensuring protection

No prosecutor would ask, and no judge would authorise the interception of people who could claim they are covered by secrecy of information in order to elicit classified information. On the contrary, when the information does not fall within the professional scope, or if the professional concerned is accused of a crime, interceptions are allowed.

For example, practice shows that it is not the defence counsel, but the accused who is the target of the interception, and this is the reason why the counsel's conversation is usually indirectly intercepted. In this case, the interception continues, otherwise it would be impossible to determine whether they are acting within the limits of a professional mandate or are going to commit crimes.

As already seen, the law is clear: the interception of communications with the counsel cannot be used in criminal proceedings (art. 103 para. 5 CPP). The problem is that the police cannot stop, delete or destroy the interception, but must transmit all the material to the prosecutor, who, at the end of the operations (or at the closing of the investigation), informs the parties who have the right to listen to the intercepted conversations. According to art. 269 CPP, all interceptions are stored until the judgment has the force of *res judicata*, but the counsel who believes

that they have been unfairly intercepted could "ask for the destruction of the records not acquired by the judge who authorised or validated the interception" in order to protect their privacy.

Art. 103 para. 7 CPP has been implemented by *decreto legislativo* no. 216 of 2017 in order to grant higher protection to defence counsels: "with due respect for the inadmissibility provided in the first paragraph, when conversations and communications are intercepted, their content cannot be transcribed, not even summarily. Moreover, the record of the operations indicates only date, time and device of the interception." This provision should have entered into force on 26 July 2018, but the Government postponed its entrance to after 31 March 2019, as previously mentioned.

4. Execution of telecommunications interception

a) Execution by the authorities with or without the help of third parties

As explained in depth (see above, para. I.A.3.), the Italian Code of Criminal Procedure gives preference to a model where interceptions should be done through the instruments available at the *Procura della Repubblica*, while the recourse to other public offices or private agencies, should be exceptional and explicitly authorised by the prosecutor (see art. 268, paras. 3 and 3-*bis* CPP for judicial interceptions; art. 25-*ter* para. 2 of *decreto-legge* no. 306 of 1992 for preventive interceptions; and art. 78 para. 2 of *Codice antimafia*, for interceptions within preventive measures referring to art. 268 CPP).

These authorisations – and the use of private agencies – are frequent when classic wiretapping is insufficient, and thus it is necessary to use high-tech interceptions, such as the *captatore informatico*.

Note the apparent paradox: in order to conduct traditional wiretapping, the judicial authority and the judicial police, despite utilising specific listening rooms, always need the cooperation of the telephonic service provider (that is a private entity), to which it requests the duplication of the targeted line. On the contrary, using a *captatore informatico*, the judicial authority and the judicial police can intercept directly from the source, without the involvement of a private service provider. The problem is that, as the *captatore informatico* is new software, they still have to ask a private party to provide it.

The support of private entities is instead used for renting, supply, and maintenance contracts related to the devices available at the *Procura della Repubblica* (see above, para. I.A.3.).

The jurisprudence has provided a solution to the question as to whether a letter rogatory is required to intercept telephonic conversations with subjects abroad. What must be considered is not the physical place where the person is located, but

the nationality of the telephonic service provider: when at least one of the two lines is Italian, it is always possible on a technical level to intercept the conversation using the so-called *instradamento* technique. This involves channeling through the national provider all the communications from the national territory to abroad and vice versa. On the contrary, when both the lines are ruled by foreigner providers, the authority must use the letter rogatory.[20]

The same approach is adopted for audio surveillance. For example, according to the *Corte di Cassazione*, if a bug is placed on a car leaving the Italian territory, no letter rogatory is required.

International judicial cooperation is a very important topic, considering the extreme mobility of people and their devices nowadays. For this reason, art. 31 of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014, regarding the European Investigation Order in criminal matters, considers precisely the case in which "the interception of telecommunications is authorised by the competent authority of one Member State (the 'intercepting Member State') and the communication address of the subject of the interception specified in the interception order is being used on the territory of another Member State (the 'notified Member State') from which no technical assistance is needed to carry out the interception." In these cases, it is therefore only necessary for the intercepting Member State to inform the competent authority of the notified Member State of the interception.

b) Accompanying powers for the execution of interception

As highlighted above, traditional wiretapping does not need any "accompanying power." On the contrary, audio surveillance in the domicile or other places benefitting from the same level of protection (such as the passenger compartment) assumes a previous violation by the police of that place in order to arrange microphones and transmitters. Procedural law does not discipline these preparatory activities (nor the removal of the instruments), but the jurisprudence has always considered these powers as implicitly belonging to the police, who cannot be considered responsible for crimes such as *violazione di domicilio*.[21]

The same applies to *captatore informatico*. Its installation in a cyber system clearly modifies it; nevertheless, the police is not responsible for any crime, as it is an accessory activity instrumental to the interception.

---

[20] See Cassazione penale, sezione I, 31-03-2009, n. 13972, in CED, rv. 243138; sezione IV, 28-03-2008, n. 13206, in CED, rv. 239288; sezione IV, 14-05-2004, n. 32924, in CED, rv. 229103; sez. V, 02-07-1998, n. 4401, in CED, rv. 211520. Among other scholars see *La Rocca*, in Giurisprudenza italiana, 2011, pp. 731 ff.

[21] See Cassazione penale, sez. II, 13-02-2013, n. 21644, in CED, rv. 255541; Cassazione penale, sez. I, 02-10-2007, Biondo, in CED, rv. 238108; Cassazione penale, sez. IV, 28-09-2005, Cornetto, in CED, rv. 232777.

5. Duties of telecommunications service providers to cooperate

a) Possible addresses of duties of cooperation

In Italy, as in other European countries (for example, Spain), the duty of the service providers to cooperate with the judicial authority in intercepting activities is imposed by law only in general terms.

This duty can even be inferred from two provisions generally ruling the activities of the assistants/advisors of the prosecutor and of the police. According to art. 359 para. 1 CPP "the prosecutor, while proceeding (…) to any other technical operation requiring specific technical competences, can appoint advisors and use their competences. The advisors cannot refuse their office." Art. 348 para. 4 CPP provides an analogous provision: "the judicial police, when, of its own initiative or according to the instructions of the prosecutor, carries out acts or operations requiring specific technical competences, can make use of appropriate individuals who cannot refuse their office."

These provisions are applicable to all cyber-communications service providers. They are subject to a functional principle: the judicial authority contacts those it believes to be the most appropriate to carry out the interception activities, and they cannot refuse their office.

b) Content of duties to cooperate

It is not only the recipients (see previous para. a.), but also the (technical) content of the duty which is not clearly identified. The contents of the duty depend on the concrete measures adopted by the authority, and therefore from the kind of investigation required. Despite not being directly linked to interceptions, the following example can be helpful: the Italian courts have reached the conclusion that when it is necessary to prevent access to a website *(oscuramento)* it is possible to use the preventive seizure outlined in art. 321 CPP. This measure orders all Italian service providers to prevent access to users.[22]

Coming back to interceptions, it is clear that the content of the duty to cooperate changes in respect of operations to be carried out. Therefore, as already mentioned (see above, paras. I.A.3. and III.B.4.a.), in most cases wiretapping and cyber-interceptions only require the service provider to duplicate the line and divert it to the CIT of the *Procura della Repubblica* making the request.

---

[22] See Cassazione penale, sezioni unite, 29-01-2015, n. 31022, in Cassazione penale, 2015, p. 3437: "in light of the proportionality principle, the precautionary seizure (ruled at art. 321 CPP) of a web-site or a single telematic page is admissible if there are the *fumus commissi delicti* and the *periculum in mora*, also by imposing to the service provider to prevent the access to the relevant web-site or telematic page."

In Italy, interception is a "dynamic" investigative means, as it requires communication between people. When the communication reaches the recipient, the instruments to be used are different, such as the search, the cyber search (art. 247 CPP) and the seizure of the communicated data relevant for the investigations (arts. 253 ff. CPP; see above, para. III.B.2.b.).

According to art. 247, para. 1-*bis* CPP, introduced in 2008: "when there is reason to believe that data, information, software or traces related to the crime are in a cyber- or telematic system, even if protected by security measures, it is possible to search adopting technical measures granting the conservation of the original data and preventing any modification."

According to art. 254-*bis* CPP, also introduced in 2008: "when ordering the seizure of data collected by providers of cyber-, telematic or telecommunications services, including traffic and geo-localisation data, the judicial authority may copy them on appropriate devices granting the regular provision of the services. The procedure must grant the conformity of the acquired data to the original ones. In this case it is nonetheless ordered to the service provider to store and adequately protect the original data."

Both these provisions aim to protect the integrity of the cyber systems to be searched and the authenticity of the data to be seized. The law does not entail any indication of the proceedings to be followed, as the rapidity of technical progress would mean that any indication would be soon outdated. A referral to the current applicable best practices is a far better solution.

c) Checks, filtering and decryption obligations of communications service providers

When operators of telecommunications services are involved in interception activities inevitably some problems rise. There are three main issues:

First of all, confidentiality. The operators, through their employees, know or at least "handle" confidential data concerning criminal investigations. They should be prevented from informing the people involved or the press.

Second, the authenticity of the data. Operators know that data can be modified, changed or affected. This is why the "chain of custody" is so important and the operators must respect some technical adjustment.

The third problem is related to the costs. The operators are companies legitimately trying to improve their profits while investigative activities invoke significant cost. The question therefore is, what are the limits within which the public authority can transfer the costs of cyber-criminal investigations to private entities? This is particularly problematic for data retention (see below, para. III.C.1.). Art. 24 of *legge* no. 167 of 20 November 2017 *(legge europea 2017)* increased to 72 months

(7 years) the mandatory time limit for operators to maintain telephonic external data for investigations related to a list of grave offences. Leaving aside the users' "right to be forgotten," the operators could object the excessive costs of this measure.

As explained in paras a. and b., the Italian legislation does not take any position on these problems. Nevertheless, the Data Protection Authority *(Garante per la protezione dei dati personali)*, a figure existing in many other European countries and at the EU level (the *European Data Protection Supervisor*, EDPS) has highlighted them.

On 15 December 2005 the Italian Authority issued pursuant to art. 154 para. 1 letter c) Privacy Code[23] some "mandatory security measures for interceptions" for the "cyber-communications service providers carrying out activities under request of the judicial authority." It mandated companies to adopt the following measures:

a) organisation of security measures:
   - adoption of organisational models minimising access to information, with a strict division of the data visibility on an organisational, functional and geographical basis;
   - selective identification of the officers authorised to handle personal data;
   - a strict control of the quality and coherence of the credentials for the access to data;
   - distinction between data of mere administrative-accounting character and documentary data to be produced;
   - strict procedure for authentication, even resorting the use of biometric features;

b) security of the flow of information to the judicial authority:
   - adoption of communication systems based on adjourned telematics instruments developed with secure web-protocols;
   - adoption of digital signature in order to encrypt documents;
   - use of encrypting tools based on the digital signature to communicate to the judicial authority the results of the accessory activities carried out;
   - use of the Internet e-mail only where certified (*Posta Elettronica Certificata*, PEC);
   - use of delivery services only if identified by the judicial authority and keeping record of the deliveries;
   - limitation of the use of unsecure means of communications only when it is technically impossible to use the more secure channels that are available.

c) data protection for reasons of justice:
   - develop of cyber-tools that ensure the control of the activities carried out on specific information available on the databases, recording the operations in a specific audit log;
   - adoption of modern encrypting instruments for data protection during their permanence in the informative-system of the provider;

---

[23] The provision states: "in addition to other specific provisions, the Authority, also through its Office and in conformity with this code: (…) c) imposes, if necessary proprio motu, the responsible for the treatment to adopt the necessary or appropriate measures in order to make the treatment consistent with the applicable law (…)." The Privacy Code can be read on the website of the Authority.

– limitation of the permanence of personal data only as required for the execution of the judicial decisions. After the communication of data to the requesting judicial authority the data must be immediately deleted.

6. Formal prerequisites for interception orders

a) Competent authorities

According to art. 267 CPP, interception activities must be authorised by the judge at the request of the prosecutor. In cases of urgency, when waiting for the authorisation of the judge would prejudice the investigative activity, interceptions can be provided by the prosecutor with a reasoned order, which must immediately or within a short time-limit be transmitted to a judge for validation.

In para. III.B.3.a.aa., as has already been highlighted, Members of Parliament benefit from some guarantees when subject to interceptions: art. 68 para. 3 Constitution requires the authorisation of the House to which the parliamentarian belongs. The detailed regime is contained in *legge* no. 140 of 20 June 2003: art. 4 states that when it is necessary to intercept a parliamentarian, both by wiretapping and audio surveillance or to ask for the phone logs, the competent authority submits a request to the House. The request is presented by the authority that issued the measure to be implemented, and the implementation is suspended whilst the authority awaits authorisation. According to art. 5, the authority explains the object of the proceedings and the allegedly violated provisions, providing the House with the reasons grounding the measure.

Special guarantees are granted also to the President of the Republic. Art. 90 Constitution provides immunity for the Head of State for acts committed in the exercise of their functions, with the exception of high treason and "attempt to the Constitution." *Legge* no. 219 of 5 June 1989, implementing the constitutional norm, states in art. 7 that it is possible to intercept the President of the Republic only in order to investigate the abovementioned crimes. Moreover, interceptions must be authorised by the Committee provided by art. 12 of the *legge costituzionale* no. 1 of 11 March 1953 and after they have been suspended from their functions by the Constitutional Court. In exceptional and urgent circumstances, the president of the Committee can authorise interceptions, but this decision must be confirmed by the panel within ten days.

Analogous provisions attaching the possibility to intercept only after the authorisation of other non-judicial constitutional institutions are provided for members of the European parliament (*legge* no. 437 of 1966 and *legge* no. 170 of 1977), the judges of the Constitutional Court (art. 3 para. 2 of *legge* no. 1 of 1948), the Prime Minister *(Presidente del Consiglio)* and Ministers, even after the end of their mandate for ministerial crimes (art. 10 para. 1 of *legge* 1 of 1989).

b) Formal requirements for applications

The law does not impose any formal conditions on the request of the judicial authority, but it must indicate the legal precondition for the authorisation and the prosecutor has a duty to attach the relevant documents and evidence for the assessment.

c) Formal requirements for orders

Interceptions are authorised by judges. The reasoning of the order must be analytical, specific, and independent, and it must adequately justify the existence of serious evidence of the crime *(gravi indizi di reato)* and the indispensability of interceptions for the prosecution of investigations.

For future interceptions with the *captatore informatico*,[24] there are some additional conditions: the order must contain the reasons justifying the need for this kind of interception and, for the crimes enlisted in art. 51 paras. 3-*bis* and 3-*quater* CPP (organised crime and terrorism), it must indicate in which places and at what time the microphone can be switched on. The identification of these last conditions can also be indirect.

In the case of urgency, when the prosecutor carries out audio surveillance through the *captatore informatico* on an electronic device for the crimes of art. 51 paras. 3-*bis* and 3-*quater* CPP, the order must also indicate the reasons of urgency making it impossible to wait for the authorisation of a judge.

7. Substantive prerequisites of interception orders

a) Degree of suspicion

This aspect has already been partially addressed while describing the general Italian "security architecture" in para. I.A.2.a. Now it will be analysed in detail.

i. According to the ordinary regime, the legal conditions supporting the authorisation are the following:

– interceptions can be authorised only while investigating the crimes enumerated in art. 266 CPP (see below);
– there must be serious evidence of the crime *(gravi indizi di reato)* and the interceptions must be absolutely necessary for the prosecution of investigations (art. 267 CPP).

---

[24] They can be realised only after 31 March 2019 (see above para. III.B.2.c.dd.).

Nevertheless, two special regimes provide lower standards:

– according to art. 13 of *decreto-legge* no. 152 of 13 May 1991, signed into law with amendments by *legge* no. 203 of 12 July 1991, for organised crimes,[25] threats by telephone, and other specific relevant crimes,[26] interceptions can be authorised if there is enough evidence of a crime and interceptions are only necessary (instead of absolutely indispensable) for the investigations;
– according to art. 6 of *decreto legislativo* no. 216 of 2017, the same regime is applicable in the proceedings of public officials against the public administration, sentenced with imprisonment to at least five years as a maximum limit.

ii. Another substantive prerequisite, linked to the degree of suspicion, depends on the type of interception and on the location where it takes place.

– Indeed, the Code of Criminal Procedure grants particular protection to conversations taking place within a private domicile. Therefore, according to the general regime and art. 266 para. 2 CP, in order to authorise interceptions within the domicile (and the other places identified by art. 614 CP) there also must be "reasonable basis *(fondato motivo)* to believe that a criminal activity is taking place there."

It is obvious that the special regimes have a different discipline:

– as far as organised crimes, threats by telephone and the other relevant specific crimes are concerned, art. 13 para. 1 of *decreto-legge* no. 152 of 13 May 1991, signed into law with amendments by *legge* no. 203 of 12 July 1991, expressly states that "interceptions are allowed even if there is no reason to believe that the criminal activity is taking place there;"
– the same regime is applicable to the crimes of public officials against the public administration thanks to the general referral of art. 6 para. 1 of *decreto legislativo* no. 216 of 2017 to art. 13 of *decreto-legge* no. 152 of 1991.

---

[25] According to a recent – and open to criticism – judgment of the *Corte di Cassazione* (Cassazione penale, sezioni unite, 28-04-2016, n. 26889, Scurato, in CED, rv. 266906) the expression *criminalità organizzata* includes not only the mafia organisations (art. 416-*bis* CP) but also the *associazione a delinquere* (art. 416 CP).

[26] Art. 3 of *decreto-legge* no. 374 of 18 October 2014, signed into law with amendments by law no. 438 of 15 December 2001, extended the applicability of art. 13 of *decreto-legge* no. 152 of 1991 to:

– crimes at art. 270-*ter* and 280-*bis* CP (insurgent and terrorist association);
– crimes at art. 407, para. 2, letter a), no. 4 CPP (crimes of terrorism).

Finally, art. 9 of *legge* no. 228 of 11 August 2003 extended the applicability of art. 13 of *decreto-legge* no. 152 of 1991 to:

– crimes at libro II, titolo XII, capo III, sezione I CP (crimes against the individuals such as enslavement, child prostitution, child pornography, etc.);
– crimes at art. 3 of legge no. 75 of 20 February 1958 (exploitation of prostitution).

Therefore, when the report refers to "organised crimes and other specific relevant crimes" it means all the crimes enumerated in this footnote.

iii. In this framework the question that arises concerns the regime applicable to the *captatore informatico* when it enters into force. The question is legitimate, keeping in mind that this instrument can be used only for audio surveillance (see above, para. III.B.2.c.dd.).

Art. 267 para. 2 CPP provides a general rule: the *captatore* can intercept conversations within a private domicile only when there is the additional condition of the "reasonable basis (fondato motivo) to believe that a criminal activity is taking place there."

Para. 2-*bis* of the same article (introduced by the *decreto legislativo* no. 216 of 2017) shows the exception: in the proceedings for the crimes of art. 51, paras. 3-*bis* and 3-*quater* CPP (organised crimes and terrorism), the use of the *captatore* is "always" admissible, therefore also within the domicile and when there is no reason to believe that a criminal activity is taking place there.

As regards the crimes of public officials against the public administration, despite the inaccurate expression, art. 6 para. 2 of *decreto legislativo* no. 216 of 2017 states: "the audio surveillance in the places enumerated in art. 614 CP cannot be done by installing the captatore informatico on a device when there is no reason to believe (motivo) that a criminal activity is taking place." The double negation should imply the applicability of the general discipline of art. 267 para. 2 CPP.

iv. Even if it is not formally part of the "degree of suspicion," the telephonic interception enabling a search for a fugitive (see above, para. I.A.2.a.iv.) pursuant to art. 295 para. 3 CPP is relevant.

The provision does not refer to serious evidence of a crime *(gravi indizi di reato)*, but it must still exist: indeed, a precautionary measure (assuming the existence of evidence against them) will be pending concerning the fugitive, or a verdict of guilt beyond reasonable doubt.

b) Predicate offences

i. According to art. 266 para. 1 CPP, the interception of telephonic or telecommunications conversations or communications is allowed in the proceedings against the following crimes:

a. non-culpable crimes punished with life sentence or imprisonment of more than five years as a maximum limit;
b. crimes against the public administration punished with imprisonment of at least five years as a maximum limit;
c. drug crimes;
d. crimes connected with arms or explosives;
e. smuggling crimes;

f. the crimes of injury *(ingiuria)*, threat *(minaccia)*, usury *(usura)*, abusive financial activity *(abusiva attività finanziaria)*, insider trading *(abuso di informazioni privilegiate)*, market abuse *(manipolazione del mercato)*, telephonic harassment or disturbance *(molestia o disturbo delle persone col mezzo del telefono)*;

g. crimes at art. 600-*ter* para. 3 CP (child pornography), even if related to art. 600-*quater*.1 CP (virtual pornography) and art. 609-*undecies* (child soliciting, *adescamento di minorenni*);

h. crimes at art. 444 CP (trade in harmful food, *commercio di sostanze alimentari nocive*), 473 CP (counterfeiting, alteration or use of trademarks or patents, models and drawings, co*ntraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni*), 474 CP (import and trade of products with false signs, *introduzione nello Stato e commercio di prodotti con segni falsi*), 515 CP (trade fraud, *frode nell'esercizio del commercio*), 516 CP. (sale of non genuine food as genuine, *vendita di sostanze alimentari non genuine come genuine*), and 517-*quater* CP (counterfeiting of information related to the geographic origin or the original name of agrifood products, *contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari*);

i. crime at art. 612-*bis* CP (stalking, *atti persecutori*).

In the same cases, audio surveillance is admissible.

According to the jurisprudence, the results of interceptions can be used also for crimes other than those enumerated in art. 266 CPP, if the authority is aware of these crimes because of the authorised interception for the abovementioned crimes. Nevertheless, a strict objective, evidentiary, and teleological link between the crimes that led to the authorisation of the investigation and the crimes incidentally intercepted must exist.

ii. It is important to remember the existence of the special regimes mentioned above at letter a), as they not only introduce a lower degree of evidence, but they are also applicable only to limited categories of crimes (organised crimes and other specific relevant crimes, crimes against the public administration, etc.).

iii. Wiretapping for the search of a fugitive pursuant to art. 295 para. 3 CPP is not linked to a specific crime the fugitive is accused of, as it is connected to the condition of the subject.

If the search for the fugitive is carried out specifically by audio surveillance, art. 295 para. 4 CPP requires the crimes to be of a certain gravity, limiting it to the crimes at art. 51 para. 3-*bis* CPP (organised crimes) and 407 para. 2 letter a) no. 4 CPP (terrorism).

c) Persons and connections under surveillance

When the law (art. 267 CPP) requires serious evidence *(gravi indizi)* in order to authorise an interception, this evidence must concern the existence of a crime and not the personal culpability of a person. In other words, proceedings can still be pending against unidentified people and the interception can be the tool for their identification (typically for crimes committed by telephone).

Moreover, not only persons under investigations, but also other people whose conversations are relevant for the investigations can be intercepted. For example, in the case of the fugitive, people who have contact with them can be intercepted and so can contribute to finding them. The law introduces a limit preventing the possibility to intercept defence counsels, private investigators, expert witnesses and their assistants (art. 295 para. 4 CPP, referring to art. 103 para. 5 CPP).

According to the jurisprudence, when proceeding against a legal person in order to assess the possible administrative responsibility caused by an offence *(responsabilità amministrativa nascente da reato)* pursuant to *decreto legislativo* no. 231 of 2001, the results of authorised interceptions of individuals during the investigation on the predicate offence may be used, even if the proceeding against the legal person becomes autonomous for procedural reasons.

Finally, according to art. 266-*bis* CPP, in proceedings against the crimes enumerated in art. 266 CPP and crimes committed through cyber- or telematic means, the interception of the flow of communications regarding cyber- or telematic systems or between additional systems is allowed. Therefore, the authorisation of the judge can target not only a person but also a specific phone number or an ID code for telephonic or telematic connection, such as an email account, the IP address or the IMEI.

d) The subsidiarity principle

The subsidiarity principle is always valid: according to art. 267 CPP, interceptions must be *absolutely indispensable* for the continuation of investigations. Nevertheless, in the proceedings for organised crime and other specific relevant crimes, the standard is lower: interceptions may be authorised even if only *necessary* for the investigations. The same principle is applicable to the crimes of public officials against the public administration, sanctioned with imprisonment of at least five years as a maximum limit (see above, letter a.).

e) Proportionality of interception in individual cases

In the Italian system, the proportionality principle is expressly mentioned in the precautionary measures regime (limitation to the individual freedom, before the final judgment). Among other criteria, art. 275 CPP imposes an obligation to

choose the measure which affects personal freedom the least. Proportionality is to be considered in relation to the offence and the possible applicable sanction at the end of the trial.

As far as the interception of communications is concerned, the principle is not expressly mentioned, and the heart of the protection is linked to the principle of legality (here as "riserva di legge formale e di giurisdizione" of art. 15 Constitution) and the principle of equality and reasonableness (art. 3 Constitution).

In respect to ordinary law, an abstract assessment of proportionality is the basis for the legislator's decision to allow interceptions only for specific crimes with a certain degree of gravity or punishable with sanctions reaching a certain degree of gravity.

As interceptions affect the right to private life and privacy, the proportionality principle in interceptions is also to be taken into account thanks to the relevance within the Italian system of the European Convention of Human Rights (art. 8) and the Charter of Fundamental Rights of the European Union (art. 52 in conjunction with arts. 7 and 8) directly recognising its importance.

f) Consent to the measure by a communication participant

Within the Italian system, interceptions assume that the person under surveillance is not aware of the interception (the so-called *clandestinità dell'intercettazione*).

If one of the people under surveillance is informed of the interception, or records the conversation, the regime is not applicable. The jurisprudence tends to qualify the recording of conversations by one of the people involved in it as documental evidence (art. 234 CPP).[27]

8. Validity of interception order

a) Maximum duration of interception order

The duration of the interception order cannot exceed fifteen days (art. 267 para. 3 CPP). In case of urgency, when there exist grounds to believe *(fondato motivo di ritenere)* that the delay could affect the investigations, the prosecutor authorises the interception with reasoned decree *(decreto motivato)* and transmits it immediately to the judge or within the following twenty-four hours. The judge, within twenty-four hours decides whether to validate the decree or not with another reasoned de-

[27] See Cassazione penale, sez. VI, 03-10-2017, n. 1422, in Foro italiano, 2018, II, column 252 (annoted by Minafra), stating that: "the record of a conversation by one of the participants to the conversation falls within the licit documental evidence, therefore it is certainly admissible (litt. utilizzabile), even if its reliability must be verified."

cree. If the prosecutor's decree is not validated in time, the activities cannot proceed and the results of interceptions cannot be used in trial (art. 267 para. 2 CPP).

In proceedings for organised crime and other specific relevant crimes (see above, para. III.B.7.a.), the duration of the interceptions cannot exceed forty days. In case of urgency, the prosecutor can authorise the operations with a decree, requiring the validation of a judge, in the same way as mentioned above.

b) Extension of authorisation

The duration of an interception order can be extended by the judge with a reasoned decree each time for fifteen days if the legal requirements still exist (art. 267 para. 3 CPP).

In the proceedings for organised crime and other specific relevant crimes (see above, para. III.B.7.a.), the duration of the interception decree can be extended by the judge with a reasoned decree each time for twenty days if the legal requirements still exist.

The law does not provide a maximum time-limit for the interception decree or a limit on admissible extensions.

c) Revocation of authorisation

As a general principle, the authorisation is revoked when the legal requirements are no longer met.

9. Duties to record, report and destroy

a) Duty to record and report

In the recent *decreto legislativo* no. 216 of 29 December 2017, the Government renewed the regime of transcription, deposit, and conservation of intercepted data, in order to further the respect of privacy.

Nevertheless, due to art. 2 para. 1 of *decreto-legge* no. 91 of 25 July 2018, the new discipline will be applicable only after 31 March 2019. Therefore, the two following paragraphs will analyse separately:

– the regime as formally amended, but still applicable until 31 March 2019; and
– the new regime, that will be applicable only after that date (and unless other amendments are approved).

aa) The applicable regime

Art. 267 para.4 CPP states that the prosecutor carries out interceptions personally or through a police officer.

The intercepted communications are recorded and a report of its content or a summary is prepared (the so-called *brogliaccio*).

Art. 268 para. 4 CPP states that the records and the report are immediately transmitted to the prosecutor. Within five days of the end of the operations, they must be filed with the secretariat of the office of the prosecutor with the decrees allowing, authorising, validating, and extending the interception. The prosecutor decides how long they have to remain there, unless the judge deems it necessary to extend the deadline. According to art. 268 para. 5 CPP, if this deposit may seriously prejudice the investigation, the judge authorises the prosecutor to delay it up to the conclusion of the investigation (and this is what usually happens).

According to art. 268 para. 6 CPP, the parties have the right to examine the results of interceptions. The provision also introduces the deadline for this purpose. After that, taking into account the requests of the parties, the judge selects the conversations or flows of cyber- and telematic communications that are not deemed manifestly irrelevant; and vice versa, deletes the inadmissible *(inutilizzabili)* records. Then, the judge orders the whole transcription of the records or the printing of the information contained in the selected flows of cyber- and telematic communications by way of a particular technical expertise (forms, modes, guarantees, etc.). The transcription or the printed copies of interceptions are collected in the trial dossier *(fascicolo per il dibattimento)*, which means they can be used in the trial.

The judge who authorised the interception is neither informed of the results of the operation, nor receives information during the activities.

bb) The regime after 31 March 2019

Art. 267 para. 4 CPP states that the prosecutor carries out the interceptions personally or through a police officer. The intercepted communications are recorded, and a report of the operation is made (the so-called *brogliaccio*), containing, even summarily, the content of the intercepted conversations.

The police officer acts pursuant to art. 268 para. 2-*bis*, informing the prosecutor in advance and noting the contents of communications and conversations.

Art. 268 para. 2-*bis* CPP prohibits the transcription, even summarily, of communications and conversations irrelevant for the investigations and relating to personal data qualified as “sensitive” by law. In this case, the report only indicates the date, time, and device used for the interception. Art. 268 para. 2 CPP states that the prosecutor, with a reasoned order, may provide the communications and conversations

of para. 2-*bis* to be transcribed in the report if relevant in trial. Where necessary, the same applies for personal data qualified as "sensitive" by law.

Art. 268 para. 4 CPP states that the report and records are transmitted to the prosecutor and collected in the private file *(archivio riservato)* immediately after the ending of the operation, which is determined by the interception order or its extension. When the investigations are complex, the prosecutor can order that the transmission of the reports and records be postponed when the continuation of operations makes it necessary for the police officer to collate their results. With the same order, the prosecutor can adopt the necessary measures in order to grant the secrecy of the non-transmitted material. This provision avoids those situations where the judicial police cannot retain the results of interceptions following the conclusion of the operation, even when it continues the interceptive activities on other devices or in other places. This avoids a problem when the judicial police need to consult the collected material.

Art. 268-*bis* CPP states that within five days of the conclusion of the operations, the prosecutor deposits the notes, the records, and reports with the orders providing, authorising, validating or extending the interception activities, creating the list of communications, conversations, and flows of cyber- and telematic information to be used in trial as evidence.

If the deposit seriously prejudices the investigation, the judge authorises the prosecutor to delay it, until the conclusion of the investigation (art. 268-*bis* para. 3 CPP).

The judge who authorised the interception is neither informed of the results of the operation, nor receives information during the activities.

b) Duty to destroy

According to art. 271 CPP, interceptions carried out outside the scope and means allowed by law are inadmissible *(inutilizzabili)* (para. 1). The same applies to interceptions relating to conversations or communications of the people enumerated in art. 200 para. 1 CPP (professional secrets), when the object is information known because of the function, office or profession, unless these people have already testified on the same facts or have spread them in other way (para. 2; see above, para. II.B.3.a.aa.).

Besides these hypotheses, the applicable regime provides that the records remain on file until it is no longer possible to appeal the judgment, which becomes final. Before that, the interested parties may ask the proceeding judge to order the destruction of the records (art. 269 para. 2 CPP). The destruction takes place under the supervision of the judge and the whole operation must be reported (art. 269 para. 3 CPP).

The *decreto legislativo* no. 216 of 2017 provides a partially different regime from 31 March 2019: the records will be filed until the judgment becomes final in the private file *(archivio riservato)* of the office of the prosecutor who requested and actioned the interceptions, and are protected by secrecy. In order to grant the respect of privacy, the people who have an interest may ask the judge who authorised or validated the interception for the destruction of the non-submitted records.

Arts. 269 and 270 CPP rule on the destiny and use of interceptions by the prosecutor, judge, and police officers (according to their competences) within the criminal proceedings. Art. 271 CPP sanctions the violation of these two articles.

In the recent past, in Italy, some espionage, industrial espionage, and "dossieraggio" activities (creating files collating all the available information on a particular subject) have been perpetrated via abusive access to public or private cyber-systems (such as telephone service providers). In these cases, the acquisition of information was illegal and had nothing to do with the regime of interceptions discussed in this chapter. Instead, it is an illicit treatment of data (that can include interceptions) usually made by private subjects, in abuse of their qualifications. These subjects do not aim to ascertain the commission of crimes, but, on the contrary, to commit crimes. For this reason, in 2006 the legislator replaced art. 240 CPP, governing the destiny of such illegally collected data.

According to art. 240 CPP, the prosecutor immediately classifies and provides for the storage of files and documents concerning data, conversations, communications, and telephonic and telematic traffic illegally obtained in a protected place. The same applies to the documents created thanks to the illegal collection of information (para. 2). It is prohibited to make copy of it in any way and in any phase of the trial, and the content cannot be used. Once the prosecutor has obtained the documents, they ask the pre-trial judge *(giudice per le indagini preliminari)* within forty-eight hours to order their destruction (para. 3). Within the following forty-eight hours, the judge schedules the hearing to be held within ten days, informing all the interested parties that they can appoint a defence counsel at least three days before the date of the hearing (para. 4). At the hearing, the judge reads the order and, if they deem that the documents, media, and acts concern data and content of conversations and communications of telephonic and telematic traffic illegally made or obtained, or documents made thanks to the illegal collection of information, provides for its destruction. The destruction is executed immediately after, in the presence of the prosecutor and the defence counsels of the parties (para. 5). The destruction is reported, and the report notes the existence of the illicit interception, detention or acquisition of documents, media, and other acts. In addition, the report indicates the ways and the means used and the subjects involved in the interception, without any reference to the content of the documents, media or acts (para. 6). The Constitutional Court intervened in this regime with judgment no. 173 of 22 April 2009 but did not undermine its substance.

10. Notification duties and remedies

a) Duty to notify persons affected by the measure

The current regime (art. 268 para. 6 CPP) provides that after the deposit of the records and the reports of the interceptions at the secretariat of the office of the prosecutor, the defence counsels are immediately informed that, within the deadline indicated by the prosecutor or extended by the judge, they can examine the acts and listen the records or take knowledge of the flows of cyber or telematic communications. After the expiration of the time limit, the judge orders the acquisition of the conversation or the flows of cyber- or telematic communications the parties have indicated not manifestly irrelevant, excluding, also *proprio motu*, records and reports whose use is forbidden. The prosecutor and the defence counsels have the right to participate in the selection and are given notice at least twenty-four hours in advance.

This regime will be supplanted by the amendments introduced by *decreto legislativo* no. 216 of 29 December 2017, the intent of which is to improve the regime related to the deposit of the documentation, the selection of the material, and secrecy. The amendments will enter into force only for interceptions made after 31 March 2019, pursuant to art. 2 para. 1 of the *decreto-legge* no. 91 of 25 July 2018.

In particular, the new discipline states that within five days of the conclusion of the operations, the prosecutor deposits notes, reports and records with the orders providing, authorising, validating or extending the interceptions. They also form a list of communications or conversations and flows of cyber- or telematic communications relevant for the trial (art. 268-*bis* para. 1 CPP). The defence counsels are immediately informed that they can examine the acts, take note of the list of communications and conversations and flows of cyber- or telematic communications, listen to the records and take note of the flows of cyber- or telematic communications (art. 268-*bis* para. 2 CPP).

Art. 268-*ter* CPP states that the acquisition of the communications or conversations used during the preliminary investigation for the adoption of preventive measures is done by the prosecutor including the reports and the acts in the dossier for preliminary investigations *(fascicolo delle indagini preliminari)*. The intercepted person takes knowledge of the interception after the notification and deposit of the order for preventive measures in the registry of the judge *(cancelleria)* (para. 1).

Outside this scenario, the prosecutor, within five days of the deposit, asks the judge to acquire the communications or conversations and flows of cyber or telematic communications stored in the private file *(archivio riservato)* relevant for the trial and included in the abovementioned list (para. 2).

The defence counsels, within ten days of the receipt of the notice of deposit, may require the acquisition of communications or conversations and flows of cyber- or

telematic communications relevant for the trial and not included in the list made by the prosecutor. They may also ask for the elimination of materials included in the list which are inadmissible or whose summary transcription in the report is forbidden. This deadline can be extended by the judge for no more than ten days, if the proceedings are particularly complicated or there is a high number of interceptions (para. 3).

In conclusion, the discipline of the CPP includes the duty to inform the defence counsels of the qualified individuals in the proceedings, i.e., the person under investigation and the victim *(persona offesa)*. However, in the case of accidental or indirect interceptions there is no duty to inform third subjects.

b) Remedies

The order of authorisation of the judge following the request of the prosecutor cannot be appealed, in light of its secrecy.

Some remedies are available in a second phase: the results of interceptions made through means other than those provided by law are inadmissible (art. 271 para. 1 CPP). Inadmissibility (*inutilizzabilità*, art. 191 CPP) is a serious procedural sanction, preventing the use of evidence created in violation of specific provisions against the accused.

c) Criminal consequences of unlawful interception measures

On the side of procedural law, it has already been highlighted that the sanction for interception carried out in a manner that violates procedural rules is inadmissibility in a criminal trial (art. 271 CPP), while for interceptions and illegal collection of personal data (*dossieraggio* and other similar activities), the instrument is art. 240 CPP, ordering "destruction under supervision."

With regard to substantive criminal law, the Italian Criminal Code includes provisions with aggravating factors if the crime is committed by a public official.

Art. 617 CP states that anybody who fraudulently takes note of a telephonic or telegraphic communication or conversation between other persons, or interrupts or prevents it, is sanctioned with imprisonment from six months to four years (para. 1). Unless it can be qualified as a more serious offence, the same sanction is applicable to whoever reveals to any public media in whole or in part the content of the communications or conversations (para. 2). The sanction is subordinate to a lawsuit *(querela)* by the victim *(persona offesa)*. Nonetheless, the prosecutor acts *proprio motu* and the sanction is from one to five years if the offence is committed against a public official or *incaricato di pubblico servizio* (another category of people usually combined with the public official but with less powers) while undertaking their duties or because of their functions or service, or by a public officer or

incaricato di pubblico servizio abusing their powers or violating the duties of their function, or by someone exercising abusively the profession of private investigator (para. 3).

Art. 617-*bis* CP states that anyone, other than those permitted by law, installing tools, means, part of tools or means in order to intercept or prevent telephonic or telegraphic communications or conversations between other people is sanctioned with imprisonment from one to four years. The sanction is imprisonment from one to five years if committed against a public official or *incaricato di pubblico servizio* while serving their duties or because of her functions or service, or by a public officer or *incaricato di pubblico servizio* abusing their powers or violating the duties of their function, or by someone exercising abusively the profession of private investigator.

Art. 617-*ter* CP states that anybody who, in order to benefit themselves or others or in order to harm others, falsely creates in whole or in part the text of a telephonic or telegraphic communication or conversation, or amends or eliminates in whole or in part the text of a real telephonic or telegraphic communication or conversation, even if only casually intercepted, is punished with imprisonment from one to four years if they use or allow others to use it (para. 1). The sanction is imprisonment from one to five years if committed against a public officer or *incaricato di pubblico servizio* while serving their duties or because of their functions or service, or by a public officer or *incaricato di pubblico servizio* abusing their powers or violating the duties of their function, or exercising abusively the profession of private investigator (para. 2).

The *legge* no. 547 of 1993 introduced some new offences into the Criminal Code whose object is the communication between cyber-systems.

Among these provisions, art. 617-*quater* CP states that whoever fraudulently intercepts communications concerning cyber- or telematic systems or between systems, or prevents or interrupts them, is sanctioned with imprisonment from six months to four years (para. 1). Unless qualified as a more serious offence, the same sanction is applicable to whoever reveals with any means for public information in whole or in part the content of the communications mentioned in para. 1 (para. 2). The punishment of these offences is subordinate to a lawsuit by the victim (para. 3). Nonetheless, the prosecutor acts *proprio motu* and the sanction is from one to five years if the offence is committed 1) against a cyber- or telematic system used by the State or another public entity or by an enterprise for public services or services of public necessity; 2) by a public official or *incaricato di pubblico servizio* abusing their powers or violating the duties of their function or service, or abusing their qualification as system operator; 3) exercising abusively the profession of private investigation (para. 4).

According to art. 617-*quinquies* CP, anyone, besides those permitted by law, who installs devices in order to intercept, prevent or interrupt communications re-

lated to a cyber- or telematics system or between systems, is punished with imprisonment from one to four years (para. 1). The imprisonment is from one to five years in the cases of art. 617-*quater* para. 4 CP (para. 2).

According to art. 617-*sexies* CP, anyone who, in order to benefit themselves or others or in order to harm others, falsely creates, modifies or delates in whole or in part the content of communications related to cyber- or telematic systems or between systems, even if only casually intercepted, is punished with imprisonment from one to four years if they use or allow others to use it (para. 1). The imprisonment is from one to five years in the cases of art. 617-*quater* para. 4 CP (para. 2).

It must be noted that, if the installation of a *captatore informatico* presumes an unauthorised access or the unauthorised presence in a cyber system, the acquisition of data and information exceeding the boundaries of law and the order of the judge or the prosecutor could constitute the offence described in art. 615-*ter* CP with aggravating circumstances. This provision states that anyone who abusively gains access to a cyber- or telematic system protected by security measures or stays there without the expressed or tacit consent of whoever has the right to exclude them, is punished with detention of up to three years. Detention is from one to five years if the offence is committed by a public official or *incaricato di pubblico servizio* abusing their powers or violating the duties of their function or service.

Finally, art. 617-*septies* CP states that anyone who, in order to harm someone's reputation or image, spreads by any means fraudulently made audio or video recordings of private meetings or of conversations, also telephonic or telematic, held in their presence or with their participation, is punished with detention up to four years.

11. Confidentiality requirements

a) Obligations of telecommunications service providers to maintain secrecy

Resuming the analysis above (para. II.B.5.), it is clear that if service providers have the duty to cooperate with the judicial authorities during interception activities, they also have the accessory and ancillary duty to maintain secrecy in relation to these activities.

This duty aims to protect not only the privacy of intercepted people (avoiding, for example, the diffusion of information to the press), but also the investigation, as interception is a secret activity (known as "atto a sorpresa") that would be useless if people are aware that they are under surveillance.

b) Sanctions against telecommunications service providers and their employees

Wiretappings occur during preliminary investigations, when the person under investigation is not aware of being intercepted. In the Italian procedural system, all the acts during preliminary investigations are covered by secrecy pursuant to art. 329 CPP. Moreover, art. 114 CPP sets out the prohibition on publication of acts and images.

Anyone revealing acts carried out during this phase, including the operator of a communications service provider (i.e., a physical person working for the operator), and in particular reveals that a person is under surveillance or the content of the interceptions, is responsible for the crime of "rivelazione ed utilizzazione di segreti d'ufficio," described in art. 326 CP.

Journalists publishing acts or documents of a criminal trial that are still protected by secrecy, are responsible for the offence *(contravvenzione)* described by art. 684 CP.

Moreover, it is possible that if an employee of the operator informs the person investigated that they are under surveillance, they perpetrate other more serious offences, such as "favoreggiamento personale" in art. 378 CP (aiding and abetting, here to be considered as an offence and not as a mode of liability).

If this is the situation in substantive law, procedural law contains art. 115 CPP, stating that, without prejudice for the sanctions provided by law, "the violation of the prohibition of publication provided by articles 114 and 329 para. 3 letter b) CPP is a disciplinary offence when the act is committed by employees of the State or other public entities or by professionals who need a special licence granted by the State." Nonetheless, it seems difficult to apply this provision to telecommunications service operators and their employees.

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

a) Collection of traffic data

aa) Relevant information

Art. 132 of *decreto legislativo* 196/2003 (the so-called Privacy Code) is the most important norm on the collection of traffic data. In its current version it states:

Art. 132 – Traffic data retention for other purposes

1. Except as provided for by art. 123, para. 2, data on telephonic traffic (…) are retained by the provider for 24 months starting from the date of the communication, in order to ascertain and punish criminal offences, while, for the same reasons, data on telematic traffic, excluding their contents, are retained by the provider for 12 months starting from the date of the communication.

1-*bis*. Data on unanswered calls, temporarily treated by electronic communication providers accessible to the public or by a public communication network, are retained for 30 days.

2. (Abolished).

3. By the date established in paragraph 1, data are acquired from the provider with a reasoned order of the prosecutor also upon request of the defence counsel of the accused, of the person under investigation, of the victim or of the other private parties. The defence counsel of the accused or of the person under investigation can ask directly to the data provider about users of the accused according to art. 391-*quater* of the code of criminal procedure, in compliance with the requirements of art. 8, para. 2 lit. f) for incoming calls.

4. (Abolished).

4-*bis*. (Abolished).

4-*ter*. The Minister of the Interior or, upon his delegation, those responsible for central administration of IT and telematics of the Polizia di Stato, Arma dei Carabinieri and of the Corpo della Guardia di Finanza, and other subjects according to art. 226, para. 1 of the application, coordination and transition norms of the code of criminal procedure (decreto legislativo 28 July 1989, no. 271) can order, even in relation to possible requests from foreign investigative authorities, providers or operators of IT or telematic services, to retain and protect, pursuant to the indicated modalities and for a maximum period of 90 days, data on telematic traffic, excluding communication contents in order to investigate preventively according to art. 226 of decreto legislativo. 271/1989, or in order to ascertain and punish specific offences. The order, extendable when necessary for a maximum of 6 months, can foresee peculiar data retention techniques and the possible unavailability of the same data from IT and telematic service providers and operators or third subjects.

4-*quater*. The provider or the IT or telematic systems operator must execute the order issued under paragraph 4-*ter*, immediately proving its compliance to the competent authority. The provider or the IT and telematic systems operator must keep the order and the acts accordingly executed confidential for the period indicated by the authority. In case of non-compliance with the duty, art. 326 c.p. is applicable, unless the circumstances require a more severe criminal offence.

4-*quinquies*. The abovementioned orders, adopted pursuant paragraph 4-*ter*, are communicated in written form, without delay and within 48 hours from the notification to the recipient, to the prosecutor, who validates them, under the required conditions. If not validated, the orders become ineffective.

5. Data processing for the purposes of paragraph 1 is carried out pursuant to the measures and precautions prescribed by art. 17 safeguarding the concerned subject, in order to guarantee that retained data maintain the same quality, security and protection requirements as online data, as well as:

a) includes specific IT authentication systems as well as authorisation systems for processors of data named in annex b);

b) (Abolished);

c) (Abolished);

d) indicate technical procedures to periodically destroy data, after the time limits in paragraph 1 have expired.

Art. 132 Privacy Code is an exception to the general rule expressed by art. 123 Privacy Code, which states that "data concerning the subscriber's and consumer's traffic, dealt by a public network provider or by an electronic communication service provider accessible to the public, must be cancelled or anonymised when they are no longer necessary in order to forward the electronic communication, except for paragraphs 2, 3 and 5;" and, in particular, that "traffic data processing strictly necessary to invoice for the contractor, or payments in case of interconnection, shall be allowed to the provider. It shall be allowed in case of dispute about the invoice or payment request for a maximum of six months, except for the additional necessary retention as an effect of a dispute also by courts of law" (para. 2).

The *decreto legislativo* n. 109 of 30 May 2008, entitled "Implementation of Directive 2006/24/CE on retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," is complementary to the general norm in art. 132 Privacy Code. Art. 3 of the *decreto legislativo* describes in detail the data which service providers have to retain:

Art. 3 – Categories of data that telephone and electronic communication operators must retain

1. Categories of data to retain for the purposes of art. 132 of the Code are:
   a) data necessary to trace and identify the source of a communication:
      1) concerning fixed network telephony and mobile telephony:
         1.1 the calling telephone number;
         1.2 the name and address of the subscriber or the registered user;
      2) concerning Internet access:
         2.1 the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;
      3) concerning Internet e-mail:
         3.1 IP address and e-mail address and possible further identifier of the sender;
         3.2 IP address and fully qualified domain name of the mail exchange host, in case of SMTP technology or any type of host relating to a different technology, used to route the communication;
      4) concerning telephony, fax, SMS, MMS via Internet:
         4.1 IP address, telephone number and possible further identifier of the calling user;
         4.2 personal data of the registered user who made the call;
   b) data necessary to trace and identify the destination of a communication:
      1) concerning fixed network telephony and mobile telephony:
         1.1 the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;
         1.2 the name(s) and address(es) of the subscriber(s) or registered user(s);

2) concerning Internet e-mail:
   2.1 the e-mail address, or any further identifier of the intended recipient(s) of the communication;
   2.2 IP address and fully qualified domain name of the mail exchanger host, in case of SMTP technology or of any type of host relating to a different technology, used to route the communication;
   2.3 IP address used for reception or for consultation of e-mail messages by the recipient, regardless of the technology or protocol used;
3) concerning telephony, fax, SMS and MMS via Internet:
   3.1 IP address, telephone number and possible further user ID;
   3.2 personal data of the registered user who received the communication;
   3.3 the number or numbers to which the call is routed, in cases involving supplementary services such as call forwarding or call transfer;

c) data necessary to identify the date, time and duration of a communication:
1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;
2) concerning Internet access:
   2.1 the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;
3) concerning Internet e-mail:
   3.1 the date and time of the log-in and log-off of the Internet e-mail service used IP address, based on a certain time zone, regardless of thetechnology and protocol used;
4) concerning telephony, fax, texts, and MMS via Internet:
   4.1 the date and time of the log-in and log-off of the Internet service ed used IP address, based on a certain time zone, regardless the used technology and protocol;

d) data necessary to identify the type of communication:
1) concerning fixed network telephony and mobile telephony: the telephone service used;
2) concerning Internet e-mail and Internet telephony: the Internet service used;

e) data necessary to identify users' communication equipment or what purports to be their equipment:
1) concerning fixed network telephony, the calling and called telephone numbers;
2) concerning mobile telephony:
   2.1 the calling and called telephone numbers;
   2.2 the International Mobile Subscriber Identity (IMSI) of the calling party;
   2.3 the International Mobile Equipment Identity (IMEI) of the calling party;
   2.4 the IMSI of the called party;
   2.5 the IMEI of the called party;
   2.6 in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;
3) concerning Internet access, Internet telephony, fax, texts, MMS via Internet:

3.1 the calling telephone number for dial-up access;

3.2 digital subscriber line number (DSL) or other end point of the originator of the communication;

f) data necessary to identify the location of mobile communication equipment:

1) the location label (Cell ID) at the start of the communication;

2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. Data to be retained can be further specified, if necessary in order to adapt to technological developments concerning the categories listed in paragraph 1, lit. a) to f), with a *decreto of the Presidente del Consiglio dei Ministri*, or from the Minister with delegation for Public Administration and Innovation, in agreement with the Ministries for EU politics, Economic Development, Interior, Justice, Economy and Finance and Defense, consulting the Guarantor for the protection of personal data.

Prior to 1 July 2017 an exceptional norm was integrated into art. 132 Privacy Code (basic norm). It was art. 4-*bis* of the *decreto-legge* 18 February 2015, n. 7, transposed with amendments in *legge* 17 April 2015, n. 43 (successively modified by *decreto-legge* 30 December 2015, n. 210, transposed with amendments in *legge* 25 February 2016, n. 21), which stated:

Art. 4-*bis* – Provisions concerning telephony and telematic traffic data

1. Telephony and telematic traffic data, excluding in any situation the contents, retained by telecommunications service operators on the date of entry into force of the law transposing this decree, together with telephony and telematic data made after that date, are retained in derogation to art. 132, para. 1 of decreto legislativo 30 June 2003, n. 196, and following amendments, until 30 June 2017, in order to ascertain and punish criminal offences listed in art. 51, para. 3-*quater* and 407, para. 2, lit. a) of the Code of Criminal Procedure.

2. Data concerning unsuccessful call attempts starting from the entry into force of the law transposing this decree, temporarily processed by service providers of electronic communication accessible to the public or of a public communication network, shall be retained until 30 June 2017.

3. Provisions of paragraphs 1 and 2 will not be applied after 1 July 2017.

Later on, the legislator issued a new exceptional provision: art. 24, *legge* 20 November 2017, n. 167 (so-called *legge europea 2017*), still in force. Its only paragraph states:

Art. 24 – Terms of telephony and telematic traffic data retention

1. Transposing article 20 of the Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA, in order to guarantee effective investigation tools considering the extraordinary necessity to combat terrorism, even at international level, in order to ascertain and punish criminal offences listed in art. 51, para. 3-*quater* and 407, para. 2, lit. a), of the Code of Criminal Procedure, the term to retain telephony and telematic traffic data and data regarding unsuccessful call attempts (art. 4-*bis*, para. 1 and 2 of decreto-legge 18 February 2015, n. 7, signed into law with amendments in legge 17 April 2015, n. 43, is fixed in 72 months, in derogation of art. 132, para. 1 and 1-*bis*, of the code concerning personal data protection (decreto legislativo 30 June 2003, n. 196)".

It is important to highlight the carelessness of the Italian legislator. As we will see, both the basic norm (art. 132 Privacy Code) and the exceptional one (art. 24 of *legge* 20 November 2017, n. 167) show serious gaps and, taken together, create a most chaotic, unsystematic framework that is also manifestly contrary to EU law.

Decreto legislativo 10 August 2018, n. 101 *(Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, after GDPR (General Data Protection Regulation) amended co. 3, co. 5, introducing art. 5-*bis*, art. 132, in accordance with art. 12 and 22 GDPR and art. 2-*quinquiesdecies decreto legislativo* 101, introducing also the new art. 132-*ter* (processing o personal data security) and 132-*quater* (information about risks).

bb) Substantive prerequisites of collection

A first gap in the Italian regulation is evident from looking at the substantive prerequisites of collection: according to art. 132 para. 1 Privacy Code, public authorities can ask service providers for traffic data "in order to ascertain and punish criminal offences." Therefore, it is enough that criminal proceedings, for any type of criminal offence, even a minor one, are underway. No minimum degree of suspicion is required against the person under investigation.

There is no "absolute necessity or indispensability for the prosecution" requirement, in compliance with the proportionality principle.

In other words, collection is always possible, under the sole condition that a criminal proceeding is underway, and this is unacceptable.

cc) Formal prerequisites of collection

As far as formal prerequisites of collection are concerned, art. 132 para. 3 Privacy Code states that the prosecutor has the power to ask for data from providers, upon issuing a reasoned order *(decreto motivato)*. The reasoning of the order can be – and usually is – very brief. The prosecutor can act *proprio motu* or even upon request for other subjects of the proceedings: the person under investigation or the victim.

In Italy, since the reform of 2000 (*legge* 397/2000), defence counsel (both of the person under investigation and of the victim) can also undertake a "defence investigation" *(investigazione difensiva)* to guarantee the suspect/defendant and carry out investigative measures. That is why art. 132 para. 3 Privacy Code allows the defence counsel, in addition to the prosecutor, to request data from providers pur-

suant to art. 391-*quater* CPP; however, this power is limited to the defence counsel of the person under investigation and the data must concern only its proper user.

Art. 132 para. 4-*ter*, 4-*quater* and 4-*quinquies* regulate the collection of data during preventive activities, which are not of concern here.

dd) Duty of addressees to disclose information

The providers, if requested by the prosecutor, must execute the request. To ignore it means, at least, to commit the offence regulated in art. 650 CP *(inosservanza dei provvedimenti dell'Autorità)*.

The consequences differ if the request is issued by the defence counsel. In this case, if the service provider does not execute the request, the defence counsel can ask the prosecutor to act (see art. 391-*quater* CPP).

As previously noted, for communication interceptions (see above, para. III.B.5.), while the law establishes a duty to cooperate for companies providing services, the security and authenticity of the processed data is left aside. The law (introduced in 2012) only states in art. 132-*bis* Privacy Code that: "providers shall establish internal procedures in order to execute the requests issued pursuant to the provisions regulating modes of access to users' personal data" (para. 1) and that "upon request, the providers submit to the Guarantor, according to her competence, information about the procedures regulated in paragraph 1, on the number of requests, on adduced legal motivations and on answers given." Therefore, it is the duty of the *Autorità Garante per la protezione dei dati personali* (Guarantor Authority for personal data protection) to supervise the conduct of the companies and to encourage the companies to set up and update internal procedures in order to execute the requests of the judicial authority in full compliance with the existing legislation.

ee) Automated procedure of disclosure

In Italy automated procedures of data disclosure (in the examined cases) do not exist yet. At the request of the prosecutor, the provider shall order the identification and extraction of the requested data and report on it. Nevertheless, the procedure is fast and the provider responds quickly.

b) Collection of subscriber data

aa) Relevant information

In Italy there is no real distinction between the collection of traffic data and the collection of subscriber data: both of them are now realised by virtue of art. 132 Privacy Code (see above).

As seen above, art. 3 of *decreto legislativo* n. 109 of 30 May 2008 describes precisely which categories of data must be retained by the operators. According to the type of communication, data on the subscriber's identity or the registered user, used IP address, email address, IMSI, IMEI, DSL, Cell-ID, etc. shall be included.

bb) Prerequisites of data collection

Both substantive and formal prerequisites are the same as those seen earlier for the collection of traffic data: see above, paras. III.C.1.a.bb. and cc.

cc) Duty of addressees to disclose information in manual and automated procedures

The service providers addressed by the order to disclose data have the duty to provide data in the same terms described above, III.C.1.a.dd. There is no automated procedure, see above, para. III.C.1.a.ee.

c) "Data retention"

The duty of data retention, for disclosure at the request of the public authorities, is one of the most questionable aspects of the regulation.

It has already been explained that in Italy the collection of traffic and subscriber data is possible for any kind of criminal offence, on the sole condition that a criminal proceeding is ongoing.

The general rule provided by art. 132 Privacy Code imposes the duty of data retention for 24 months (para. 1); in the case of missed calls only, data need only be retained for 30 days (para. 1-*bis*). The following art. 24 of *legge* n. 167 of 20 November 2017 (so-called *legge europea 2017*), includes an exception: it raises the duty to retain all data, including missed calls, to 72 months (6 years), in order to combat organised crime offences, terrorism, and other serious criminal offences.[28]

The combination of these two norms generates aberrant consequences: in practice the service provider, who cannot know if its customers are likely to commit serious crimes (the "72 months" category) or common offences (the "24 months" category) or will not commit any offence, will end up having to retain the data of all its customers for 72 months for reasons of caution. Furthermore, for service providers, the duties to retain (at least the ones imposed by art. 132 Privacy Code) are specifically sanctioned. Art. 162-*bis* Privacy Code states:

---

[28] The list of these offences can be found in two provisions of the criminal code: art. 51 para. 3-*quater* and art. 407 para. 2 letter a) CPP

Art. 162-bis – Sanctions on the matter of retention of traffic data

1. Unless the fact can be qualified as a more serious offence and except for art. 5, para. 2 of the *decreto legislativo* transposing Directive 2006/24/CE of the European Parliament and the Council of 15 March 2006, in case of violations of art. 132, para. 1 and 1-*bis*, an administrative pecuniary sanction in the amount of 10,000 euros to 50,000 euros is applied.

Art. 5 para. 2 of *decreto legislativo* n. 109 of 30 May 2008 provides in turn:

2. Unless the fact constitutes an offence, the omission or incomplete retention of data according to art. 132, para. 1 and 1-*bis* of the Code is punished with an administrative pecuniary sanction from 10,000 euros to 50,000 euros, which can be increased by up to three times owing to the economic situation of the responsible for the violation. In case an IP address is assigned, which does not enable an unequivocal identification of the user or subscriber, an administrative pecuniary sanction from 5,000 euros to 50,000 euros is applied, which can be increased by up to three times owing to the economic situation of the responsible for the violation. Violations are challenged and sanctions are applied by the Ministry for Economic Development.

In conclusion, it is necessary to highlight some gaps in the Italian legislation on the collection of traffic data, subscriber data, and data retention, especially in light of European Union law.

Indeed, art. 132 Privacy Code transposes Directive 2006/24/CE on retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC. Directive 2006/24/CE was then declared wholly invalid by the Court of Justice of the European Union (CJEU) with the well-known Grand Chamber judgment of 8 April 2014, in joined cases C-293/12 *(Digital Rights Ireland LTD)* and C-594/12 *(Kärntner Landesregierung)* for the violation of arts. 7 *(Respect for private and family life)*, 8 *(Protection of personal data)*, and 52 para. 1 (proportionality principle) EUCFR. This judgment was then confirmed by the following CJEU Grand Chamber judgment of 21 December 2016 in joined cases C-203/15 (*Tele 2* and *Sverige AB*) and C-698/15 *(Secretary of State for the Home Department)*.

In the light of the statements of the CJEU, the Italian regulation of data retention is itself not complicit with arts. 7, 8, 52 para. 1 EUCFR, as:

– it allows the collection of traffic and subscriber data concerning every kind of criminal offence, instead of identifying restricted areas of serious criminality;
– it does not require any standard of proof for its performance (i.e., serious evidence of a crime), nor does it foresee any further substantial requirement with a limiting function (i.e., the absolute necessity to continue investigations);
– it imposes on service providers duties of data retention which are disproportionate.

As yet, no stance has been taken by the Italian courts and the problem seems to be perceived only by scholars.[29]

---

[29] *Flor*, Diritto penale contemporaneo, pp. 356 ff.; *Ruggieri*, Cassazione penale, 2017, pp. 2483 ff.; *Marcolini*, Cassazione penale, pp. 778 ff.

2. Identification of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

a) Identification of device ID with the help of IMSI-catchers

Identification of device ID via IMSI-catchers is an investigative measure which does not exist in the Italian criminal procedure system.

Information on the device ID (IMEI) and card numbers (IMSI) can be obtained by collecting traffic and subscriber data: pursuant to art. 3 of *decreto legislativo* n. 109 of 30 May 2008, IMSI and IMEI are considered to be part of the data which the service providers have the duty to retain, as they concern calls made by their users (see above, III.C.1.a.aa.).

This is also applicable to location determination. Amongst the external data which the provider has the duty to register and retain, there is also the cell-site to which the user connected during the conversation, the so-called Cell ID (see art. 3 of *decreto legislativo* n. 109 of 30 May 2008). Geo-localisation through Cell ID is approximate, because cell-sites can cover vast areas and mobile phone could be located at any point in this area.

b) Location determination via "silent SMS"

This procedure is also unknown in the Italian criminal procedure system.

The IMSI-catcher and the "silent SMS" topic requires a point already illustrated above, among the general principles (paras. II.B.1. and 2.) to be taken up once more.

On the one hand, Italian legislation does not address these two investigative acts (as a matter of fact, there are many investigative acts that are not governed by the Italian legislation); on the other hand, the practice of foreign legal systems (i.e., the German one) shows that they are technically practicable and useful as well. What if these means, even if not foreseen by the legislator, are still employed in an investigation? Despite the traditional theory, according to which it is permissible in investigations to utilise "atypical" investigative activities, nowadays the correct conclusion is to recognise a constitutional prohibition.

If public powers could freely carry out investigative activities not grounded in law which restrict a citizens' right to privacy, this right would end up being far from inviolable. In the absence of a regulation and as a consequence of the lack of any legal limitation, the act would be possible for any kind of criminal offence, without any substantive requirement, for any period of time, by any kind of public authority (also the police), without any procedural rule and without any sanction in case of infringement. This scenario is of course unacceptable.

For example, consider the monitoring of the movements of a person under investigation through GPS (or through their mobile phone, or placing a GPS without

their knowledge in their car). This act, very similar to localisation through "silent SMS," ends up being a form of (electronic) tailing and is therefore excluded from the discipline of conversation or communication interception. According to the jurisprudence, it should be classified as an "atypical" investigation act (art. 189 CPP). Consequently, it should be fully legitimate even if done at the initiative of the judicial police, in the absence of any preventive authorisation of the judge or the prosecutor. Similar results underline the unacceptable sacrifice of constitutionally relevant rights of the citizen without any fixed legal rule.

D. Access to (Temporarily) Stored Communications Data

1. Online searches with the help of remote forensic software

a) Lack of powers in the law of criminal procedure

The *captatore informatico*, intended as software suitable for any kind of use (see above, III.B.2.c.dd.), can be installed in any kind of device, portable or mobile, in order to make a "one time copy" of data contained in the device at a certain moment, or "online surveillance" that extends over a period time.

The topic has been fully examined by German scholars and jurisprudence, i.e., the "online Durchsuchung."

In Italy, the possible use of this software, wrongly named online searching, has been discussed extensively among scholars.[30] The *Corte di Cassazione*, however, has never ruled on the issue.

The use of the abovementioned software is aimed at copying or surveillance without the knowledge of the owner of the device.

In Italy there is no regulation concerning this investigative tool and therefore the matter goes back to the general problem handled above (see above, paras. II.B.1., 2., and III.C.2.b.), on the possibility of using atypical investigative acts. As a general rule, this should be forbidden, especially if it implies restrictions to or sacrifices of the person under investigation's fundamental rights.

b) Utilisation of data attained for preventive purposes in criminal proceedings

The use of programmes to perform a "one time copy" or "online surveillance" has no legal basis in criminal procedure, or in preventive investigations.

As previously explained (see above, para. I.A.3.), the field of preventive investigations is opaque. However, in principle every preventive investigative act is still

---

[30] See *Signorato*, Giappichelli, Torino, 2018, pp. 291–295; *Trogu*, in Scalfati (eds.), Giappichelli, Torino, 2014, pp. 431 ff.

aimed at crime prevention and the acquired elements cannot be used in criminal proceedings. Therefore, the use of data attained for preventive purposes in criminal proceedings is strictly forbidden.

2. Search and seizure of stored communications data

a) Special provisions

Italy ratified the Budapest Convention on Cybercrime, signed on 23 November 2001 in Budapest. The Parliament approved *legge* n. 48 of 2008 which, other than ratifying the Convention, introduced the necessary amendments in the national system in order to comply with the Convention.

The traditional regime on inspections (arts. 244 ff. CPP), search (arts. 247 ff. CPP), and seizure (arts. 253 ff. CPP) was extended to IT objects, creating at the same time gaps in the legislation. This move was undoubtedly effective in terms of energy savings, despite scholars' criticism.

For search and seizure art. 247 para. 1-*bis* CPP (see above, III.B.5.b.) states:

> When there is reason to believe that data, information, software or traces related to the crime are stored in a cyber- or telematic system, even if protected by security measures, a search is possible adopting technical measures granting the conservation of the original data and preventing any modification.

In the Italian criminal procedure system, the search is always oriented on the handover or seizure of an identified object. Therefore, even legislation on seizure, modified by *legge* n. 48 of 2008, comprehends IT data as a possible object (arts. 254 and 254-*bis* CPP).

b) Applicability of seizure provisions to electronic data

aa) Underlying principle

As previously stated, the ad hoc provision on cyber search (art. 247 para. 1-*bis* CPP) is incorporated into the traditional search regime.

The lack of specific norms imposes the application of general rules on search: for example, those concerning the regime of the competent authority (the judge or the prosecutor), the form of the reasoned order, terms, and modalities.

Among the many consequences of this asset, it is important to note that cyber search and seizure are not secret: a copy of the order of the search must always be handed over to the person involved (arts. 249 and 250 CPP).

bb) Collection of electronic communications data

(1) Stored messages before and after transmission with local storage as well as during transmission

It has already been clarified (see above, III.B.5.b.) that in Italy communications interceptions have a "dynamic" character as they assume that the communication is still ongoing.

As a result, the search of communications data before or after it has been sent can be done through the different regime of search and subsequent seizure, and not the more complicated regime of interceptions.

(2) Communications data temporarily or permanently stored with third parties for the purpose of further transmission or safekeeping

If communications data sought by the judicial authority is located on devices owned by a third party (and not by the person under investigation), i.e., on a cloud, art. 254-*bis* CPP comes into consideration (see above, III.B.5.b.):

> The judicial authority, when ordering the seizure of data collected by providers of cyber- or telematics or telecommunication services, including traffic and geo-localisation data, may be done by copying them on appropriate devices with the aim to grant the regular provision of the services. The procedure must grant the conformity of the acquired data to the original ones and that they are inalterable. In this case it is nonetheless ordered to the service provider to store and adequately protect the original data.

The limit of this norm is related to the chance for the provider to cooperate: the traditional telephonic service provider has its seat in Italy and is subject not only to Italian legislation, but also to Italian jurisdiction. However, cloud or other web service providers (i.e., email services) have no main seat in Italy or offer only minor collaboration.

c) Different standards of protection for stored and for transmitted data

Undoubtedly ordering an interception is more onerous than ordering a search.

Recalling and comparing different aspects already explained in this report:

- Interception is possible only for a limited number of pre-determined criminal offences, requires *serious evidence* (or *sufficient evidence* in the case of organised crime or assimilated criminal offences) and proportionality (indispensability or usefulness of prosecuting investigations). Moreover, and this is perhaps the most relevant aspect, an interception can only be requested by the prosecutor, and it must then be authorised by the judge. Only in case of urgency can the initiative be taken by the prosecutor and it must, however, be immediately validated.
- Search and seizure can be made for any kind of criminal offence, and does not require particular standards of proof, but only a *grounded reason to believe* that

the searched object is on a certain person or in a certain place. The "judicial authority" is empowered to issue the order: this expression encompasses both the judge and the prosecutor. As a consequence, in the course of investigations the prosecutor can autonomously decide if and when to order a search and the subsequent seizure.

d) Open and clandestine access to stored data

Only interceptions are "clandestine," that is to say realised with the person under surveillance being unaware of it.

Search is always done after having shown the interested person (who is not always the person under investigation) a copy of the search order. However, in the case of an online search ordered at the provider's seat, the copy of the order is given only to the provider, except when the accused is there during the search.

The guarantees of the defence occur later: according to art. 366 CPP, no later than three days after the act, the prosecutor must deposit in their office the transcripts of the acts (in this case the search and seizure transcripts) and they must give notice to the defence.

3. Duties to cooperate: production and decryption orders

In Italy there is no legal regulation of the order to cooperate for decoding encrypted data or for giving necessary passwords. Evidently, passwords are held both by the service provider and the private user. Imposition on the service provider to reveal, upon request, passwords and other codes to the judicial authority could be considered at the same time a disproportionate and an inevitably ineffective measure. It is in fact useful to recall the case of the contrast between FBI and Apple, in which FBI requested the codes to unlock the iPhone of the perpetrators of the San Bernardino massacre and Apple repeatedly refused to give them.[31]

Even from this perspective the utility of the *captatore informatico* is self-evident: it could manage many of these tasks, if secretly installed on the device of the interested person.

---

[31] For a newspaper review of the facts see http://www.lastampa.it/2016/02/18/tecnologia/la-guerra-fra-apple-e-fbi-spiegata-in-punti-mw1UpW6qvFe4YMyJ8M0BcO/pagina.html

IV. Use of Electronic Communications Data in Judicial Proceedings

1. Use of electronic communications data in the law of criminal procedure

In order to answer to this question, it is necessary to identify the kind of evidence or the investigative tool under consideration.

i. First of all we will consider the interception of communications (arts. 266 ff. CPP).

Interceptions are used both during investigations, for example, in order to support the request for preventive measures, and in trial in order to assess criminal responsibility. This second approach is governed by art. 431 para. 1 letters b) and c) CPP, stating that all the records of the prosecutor and police's one-off activities *(atti irripetibili)* must be introduced in the trial dossier *(fascicolo per il dibattimento)*. Interceptions are a plain example of a one-off activity.

The legal framework for the use of interceptions in trial has already been described above, considering both the discipline applicable until 31 March 2019 and after this date (see above, paras. III.B.9. and 10.). Nevertheless, there are some other aspects that should be analysed.

According to art. 268 CPP, intercepted communications are recorded and accompanied by a written record. The record contains, even summarily, the content of the intercepted communications. This is the so-called *brogliaccio d'ascolto* and it can still be used during preliminary investigations, for example, to adopt preventive measures limiting individual freedom, while it is inadmissible in trial but for the consent of the interested parties.

The submission of evidence in trial "in contraddittorio" (i.e., following the adversarial model) is a basic principle in Italian criminal procedure, unless otherwise provided. One of these exceptions is the consent of the accused, as recognised by the Constitution at art. 111 para. 5, when they decide to follow the summary judgment *(rito abbreviato)* or a plea bargaining procedure *(patteggiamento)* or gives their consent to unilateral acts, such as investigative acts. Besides these exceptions, it is not possible for a judge to base a judgment on the informal transcription of interceptions using the records of the judicial police.

Usually, only the transcription of records made following the regime for the expert report *(perizia)* can be used as evidence in trial. According to the relevant provisions (art. 268 paras. 6, 7, and 8 CPP), the counsels are immediately informed that the records have been filed at the secretary of the prosecutor, and they can access and examine the acts and listen to the recordings. Upon request, the judge authorises the submission of interceptions that are not deemed manifestly irrelevant or inadmissible. This procedure leads to the *udienza di stralcio*, a hearing during the preliminary investigations where the judge orders the transcription of the rele-

vant records to be submitted. These transcripts are filed in the trial dossier *(fascicolo per il dibattimento)* and can be used in the assessment of criminal responsibility. The counsels can obtain a copy of the transcript and the audio-recording.

As already noted, this regime has been superseded by the *decreto legislativo* no. 216 of 29 December 2017, that will be applicable only to interceptions after 31 March 2019 due to art. 2 para. 1 of *decreto-legge* no. 91 of 25 July 2018. One of the main purposes of the new regime is to rapidly "delete any reference to people only occasionally involved in the communication and irrelevant material, preventing the spread of relevant data related to people unrelated to the scenario that justifies the interception."[32]

In particular, the regime provided by the recent arts. 268-*bis*, 268-*ter*, 268-*quater* and the new version of art. 269 CPP that will be applicable from 1 April 2019 states that the judicial police must send the written and audio-records to the prosecutor immediately after the deadline for the execution of the interceptions in order to be stored in the secret file *(archivio riservato)*, and not in the trial dossier. This procedure should grant increased privacy. Then, the prosecutor has the onus to decide whether to file the documents within five days from the conclusion of the interceptive activities or, as is usually the case, to submit a request to the judge for preliminary investigations to be authorised, postponing the filing of the conclusion of the investigations, should the filing prejudice the proceedings. With regards to written and audio-records, the prosecutor must also file the notes challenging the relevance of the records made by the judicial police and transmitted to the prosecutor before the transcription of specific interceptions. The prosecutor is asked to create the list of the interceptions they deem relevant as evidence. This list is then transmitted to the judge for preliminary investigations with the request for authorisation to file its content in the dossier of the investigation *(fascicolo per le indagini)*.

Another innovation of the new framework applicable from 1 April 2019 is the removal of the *udienza di stralcio* that will be replaced by the mechanism for filing interceptions in the dossier of the investigation. After the deposit of the documents related to the interception activities, it is the prosecutor's responsibility to initiate the procedure for the submission. Unless a preventive measure has been authorised,[33] art. 268-*ter* para. 2 CPP states that within five days the prosecutor shall

---

[32] This formula is used in the explanatory report of the *legge di delegazione* no. 103 of 23 June 2017 (Legge Orlando), available at http://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0472bis_F001.pdf&leg=XVII

[33] In this case the submission of communications or conversation founding the adoption of the measure is ordered directly by the Prosecutor, who files the records and the other relevant documents in the *fascicolo delle indagini preliminari*. When they request the adoption of preventive measures, the prosecutor submits the records of the relevant conversations pursuant to art. 268 para. 2 CPP. The decision *(ordinanza)* issued by the judge is communicated to the prosecutor pursuant to art. 92 disp. att. CPP, who in addition receives

submit the request for admission of communications, conversations, and flows of cyber- or telematic conversations contained in the list they prepared and give notice to the defence. With the submission, the prosecutor discloses to the defence the whole interceptive operation and illustrates the list of documents and records they intend to introduce in the dossier of the investigation. Within ten days of this notice, the defence may ask to examine the communications or conversations and flows of cyber- or telematic communications which it deems necessary for evidentiary purposes that are not included in the prosecutor's list. The defence may also ask for the suppression of inadmissible items or items whose summary transcription is forbidden. The parties may have written exchanges on the items they want to add to or exclude from the list under the adversarial principle. Five days from the presentation of the requests, the judge, who can also listen to the recordings of conversations and communications, issues a decision adopted *in camera di consiglio* (i.e., without the prosecutor and the defence) to submit the conversations and communications chosen by the parties unless they are manifestly irrelevant. The judge also orders, possibly *proprio motu*, the exclusion of inadmissible audio and written records. Therefore, the judge usually issues the decision without scheduling a hearing and on the basis of the written requests and responses. Where necessary, the decision is issued after a hearing scheduled for the fifth day after the deadline, giving due notice to the prosecutor and the defence. The documents and records to be submitted are collated in the dossier of the investigation and the defence has the right to receive a copy. Conversely, the other items are sent to the prosecutor who stores them in the secret file *(archivio riservato)*.

According to the new regime, when the documents from the interceptions are deposited at the secretariat of the prosecutor, the defence has the right to examine and retain a copy of all the documents and to listen to the recordings. The defence has access even to the secret file and can listen to all the interceptions related to the proceedings. Such access is governed by art. 89-*bis* paras. 3 and 4 disp. att. CPP, providing that each access is noted in a dedicated cyber-logbook with date, time of entrance and departure and the consulted documents. The defence can listen to the recordings with the devices available but cannot have a copy of the stored records. This procedure aims to prevent the illicit circulation of irrelevant or inadmissible interceptions. Ultimately, art. 493-*bis* CPP establishes that the transcription of intercepted conversations, according to the regime of the expert report *(perizia)*, can be requested in trial.

Two other aspects developed by the jurisprudence in relation to the actual regime that will be likely also be applicable after 31 March 2019 must be highlighted.

The Italian *Corte di Cassazione* clarified that the transcription of telephone recordings is a mere material activity that does not require any specific technical or

---

back the documents containing the intercepted communications and conversations deemed irrelevant or inadmissible to be stored in the secret file.

scientific ability. Therefore, when art. 268 para. 7 CPP refers to the procedure and the guarantees of the expertise, it only aims to ensure that the transcription is conducted in the best possible manner. It is therefore not possible to challenge an admissibility problem of transcription per se, it is only possible to object on the grounds of a lack of correspondence between the original content of the records and the transcripts.

The evidence is made of the audio-records, and the judge can listen to their content using a device, irrespective of the transcription, which is a mere graphical transposition of the interceptions. It falls within judicial discretion to decide whether expertise is required or whether it is enough to listen to the recordings of the intercepted communications in trial or *in camera di consiglio*. The parties retain the possibility to listen to the interceptions and ask for a copy in order to make observations. As a consequence, for telephone tapping it is not mandatory to question as a witness the person who transcribed the records under the judge's request: the referral contained in art. 268 para. 7 to "the form, the procedure, and the guarantees" of the expertise only aims to guarantee the rights of the defence to participate in the transcription activities.

As far as their probative value is concerned, it has been said that self-incriminating statements legally intercepted are valid, thanks to the inapplicability of arts. 62 and 63 CPP. Therefore, these statements cannot be compared to self-incriminating declarations given to the prosecutor or the judicial police. The audio and written records of conversations are also not comparable to indirect testimony on the declarations of the accused, as there is no intermediary.

The content of the intercepted communications can also be proven through testimony as the transcript under the expertise regime is not necessary. It is obvious that the interested party can always challenge the testimony and submit the real content of the recordings. But when the conversations are inadmissible (*inutilizzabili*: see below) it is not possible to request that those who listen to the telephone conversations testify, or the exclusionary rule would be circumvented.

i. The abovementioned regime of interception of conversations is partially applicable also to cyber search (art. 247 para. 1-*bis* CPP). Cyber search, like a traditional search, is a one-off activity, therefore the records of the operations are filed in the trial dossier *(fascicolo per il dibattimento)* according to art. 431 para. 1 letters b) and c) CPP and can be used in order to assess criminal responsibility.

The only procedural rule specifically referring to cyber search is art. 247 para. 1-*bis* CPP, including "technical measures to ensure the storage of the original data and to prevent modification."

Frequently, in addition to the submission of the records, the police officers who made the search are summoned to testify.

ii. The same applies to the seizure of cyber-data (Art. 254-*bis* CPP). Similarly, for this type of operation there is a record which can be submitted in trial according to art. 431 para. 1 letters b) and c) in light of the one-off nature of the seizure.

As for the search, art. 254-*bis* CPP also mandates that the procedures must ensure conformity of the data with the original and that it is not modified.

The object of the seizure is the *corpus delicti* or a *cosa pertinente al reato* (i.e., something connected to the offence), as provided by art. 253 CPP and as such, it can be subject to further analysis. For example, a laptop may be subject to expert scrutiny in order to produce the relevant data for the trial.

iii. The submission of traffic and subscriber data in trial (data retention) must be conducted in accordance with art. 132 Privacy Code (see above, para. III.C.1.).

According to the jurisprudence, electronic or written media providing the traffic data that the service provider draws from its file may be submitted in trial and used as documentary evidence (art. 234 CPP).

iv. Ultimately, it is useful to remember that in Italy, it is also possible to submit atypical evidence not governed by the law due to art. 189 CPP.[34] Electronic evidence is often submitted through this provision. There is little more to add on this point, except to refer to the general debate on the scope and limits of art. 189 CPP in the Italian criminal system.

2. Inadmissibility of evidence as a consequence of inappropriate collection

Usually, in any system, the best way to discourage the violation of the provisions on evidence is to prevent the admissibility of evidence obtained in violation of the evidence regime. The exclusionary rules developed in the Anglo-Saxon system are well known.

The Italian Code of Criminal Procedure of 1988 was – at least originally – inspired by adversarial principles. Therefore, it foresees a general provision on the inadmissibility *(inutilizzabilità)* of evidence at art. 191 para. 1 CPP, stating that "the evidence obtained in violation of the rules provided by law are inadmissible."

In addition to this general provision, the code also includes other specific provisions on inadmissibility that deserve to be analysed.

i. The interception of conversation is ruled by art. 271 CPP stating that the following interceptions are inadmissible:

---

[34] This provision states that "when the evidence is not ruled by law, the judge may authorise its submission if it is suitable to the ascertainment of the facts and it does not put in danger somebody's moral freedom. The judge authorises the submission after consultation with the parties."

– interceptions made in ways other than the cases and procedure provided by the law (art. 271 para. 1 CPP);
– interceptions that fail to respect the procedures and guarantees of arts. 267 and 268 paras. 1 and 3 CPP (art. 271 para. 1 CPP);
– interceptions of conversations between people bound by professional secrecy when the object is the information known because of their profession or office, unless they have already spoken of the same facts or have spread them in any other way (art. 271 para. 2 CPP);
– data acquired during the preliminary operations to install the *captatore informatico* on a device and data acquired outside the time and place limits fixed by the authorisation order (art. 271 para. 1-*bis* CPP).

Irrespective of the phase or level of the trial, the judge orders the destruction of the inadmissible documents for the abovementioned reasons, unless they represent the *corpus delicti* (art. 271 para. 3 CPP).

The referral to arts. 267 and 268 CPP leads to specific procedural duties whose violation determines the inadmissibility of the evidence. There is a lot of jurisprudence on this issue: the risk of ruining long and complex interceptive operations concerning serious offences of organised crime for a mere procedural mishap is high, but it is the indispensable price of the exclusionary rules protecting the authenticity of the evidence (in this case interceptions).

ii. With regards to cyber search, the law does not provide specific procedural sanctions. In particular the abovementioned provision imposing the adoption of "technical measures aiming to grant the storage of the original data and to prevent their modification" (art. 247 para. 1-*bis* CPP) is not protected by any explicit and specific sanction.

iii. In particular the jurisprudence does not seem have declared the existence or lack of adequate "technical measures" to have an impact on the operations leading to the inadmissibility of evidence according to art. 191 CPP.

Therefore, this question is part of the wider problem of the consequences of an illegitimate search (see below for the seizure discipline). Nevertheless, a recent judgment of the ECtHR of 27 September 2018, *Brazzi vs Italy* (no. 57278/11), revealed the non-compliance with art. 8 ECHR of the Italian search regime, as it lacks an efficient preventive or subsequent judicial control. The debate surrounding the judgment in the next few months will be helpful in order to understand the consequences of this declaration.

iv. The debate on illegitimate search leads us to the question on the consequences of an illegitimate seizure. As for the search, in the absence of a specific sanction, we must refer to the general rule.

It is well known that seizure is the natural consequence of a successful search. The question that rises in any system is whether the vices of an illegitimate search

have an impact on the following seizure determining the inadmissibility of the evidence.

The Anglo-Saxon system represents an important model for this, because it developed the well-known "fruit of the poisoned tree" doctrine, extending the illegitimacy of the search to the seizure and determining the inadmissibility of such evidence. It is true that this rule is sometimes tempered by a large number of exceptions.

Conversely, the Italian jurisprudence, following the continental approach grounded on the *brocardo* "*male captum, bene retentum*," has always declared that malpractice in the preliminary search activity does not make the following seizure inadmissible. Possible consequences are criminal sanctions or disciplinary measures for the people responsible for the illegitimate conduct.

v. There is no specific provision on the inadmissibility of illegitimate data retention. Therefore, the general rule of art. 191 CPP is applicable.

This does not mean that there is no jurisprudence on this topic: for example, it has been said that "phone traffic data on phone records obtained after the deadline provided by art. 132 of *decreto legislativo* no. 196 of 30 June 2003 are pathologically inadmissible because the service provider is prohibited from storing this data in order to ascertain the commission of crimes after that date."[35]

vi. There is also no specific provision on evidence with electronic content introduced in trial as atypical evidence according to art. 189 CPP. Again, it is necessary to refer to the general function of this provision and the related jurisprudence.

3. Use of data outside the main proceedings

a) Data from other criminal investigations

The question discussed in this section is the possibility of using in a certain proceeding data collected in another proceeding. Nevertheless, with regard to the interception of communications, it is better to consider the problem from the opposite point of view, that is to say whether interceptions made in one proceeding can be exported to another criminal trial, as this is the perspective adopted by the Italian legislator. Art. 270 CPP is entitled: "utilizzazione in altri procedimenti" (use in other proceedings).

According to this provision, the results of interceptions cannot be used in other proceedings, unless they are indispensable for the ascertainment of the offences where an on-the-spot arrest is mandatory (para. 1). This is clearly a restrictive pro-

---

[35] In the same sense, see Cassazione penale, sezione V, 25-01-2016, n. 7265, Nucera, in CED, rv. 267144; Cassazione penale, sezione V, 05-12-2014, n. 15613, Geronzi, in CED, rv. 263805.

vision that aims to limit the circulation of interceptions among trials; otherwise, the protection of the defence's rights in the subsequent trial would be at risk. The on-the-spot arrest requirement stems from art. 380 CPP.[36] In these cases, the written and audio-records are deposited with the authority competent for the second trial (para. 3). The legislator introduced a specific provision for the *captatore informatico*, stating that "the results of audio surveillance made through the captatore informatico on laptops cannot be used as evidence of crimes other than the crimes leading to the authorisation order, unless they are indispensable for the ascertainment of on-the-spot offences" (para. 1-*bis*).

The jurisprudence provides a definition of "different trial" as a trial arising from a notice of an offence concerning a fact different from the object of investigation in the first, possibly linked, trial. The diversity of the trial must be assessed pursuant to material elements, therefore it is not determined by the number assigned to the notice of offence *(notizia di reato)* in the dedicated dossier, but by the content of the notice, that is to say by the factual object of investigations leading to the prosecution. The natural consequence of this definition is that "different trial" does not include investigations strictly linked to the crime prosecuted in the first trial. The Italian *Corte di Cassazione* stated that when the link between two offences (as separate historic facts) is merely casual *(meramente occasionale)* the criminal trials must be considered separate trials.

The jurisprudence allows the use of authorised interceptions of conversations involving a physical person while ascertaining the predicate offence in trials focused on the responsibility of legal persons prosecuted according to *decreto legislativo* no. 231 of 2001, even if the trial against the legal person was separate.

Any other evidence or investigative means (search, seizure, data retention, etc.) is devoid of a special discipline. The only relevant provision for knowing when evidence is admissible in a different trial is the general rule of art. 238 CPP.

b) Data from preventive investigations

The different possibilities of preventive interceptions have already been taken into consideration (see above para. I.A.2.b) and c). Nevertheless, we must remember that almost all the proactive investigative activity is governed by the general discipline provided by art. 266 para. 5 disp. att. CPP, stating that "in any case, the elements obtained through preliminary activities cannot be used in criminal proceedings but for investigative purposes. In any case preventive interceptions and the information obtained throughout cannot be mentioned in investigative acts, object of files or otherwise disclosed."

---

[36] The legislator could extend the list and circumvent the restriction provided by art. 270 para. 1 CPP and the appetite for doing so has increased in the last ten years.

It is well known that these activities can be realised with a limited number of guarantees and controls. Allowing extensive preventive activities and then authorising their transfer and use in criminal proceedings and trials would overturn the system.

The clause "but for investigative purposes" has nevertheless been interpreted in different ways, in particular with regard to the possibility to refer this investigative activity not only to prevention but also to the following criminal investigations. Recent jurisprudence has denied any use of preventive interceptions within a criminal proceeding; the only limited use is the possibility that a preventive interception contains a notice of offence relevant for the opening of a formal investigation.

c) Data obtained from foreign jurisdictions

With regards to data coming from foreign jurisdictions, in partial anticipation of what will be discussed below in section V. we will explain the peculiarities of the Italian system when judicial cooperation in criminal law comes into consideration.

Cooperation among EU States is primarily governed by EU law, in particular Directive 2014/41/UE of the European Parliament and Council of 3 April 2014 on the European Investigation Order (EIO) transposed in Italy through *decreto legislativo* no. 108 of 2017. Within the limits provided by EU law, international, bilateral or multilateral conventions signed by the Member States are applicable. One example is the European Convention on Mutual Assistance in Criminal Matters signed in Strasbourg on 20 April 1959. In the unlikely event that the requested judicial assistance is not governed by EU law or international conventions the provisions of the *Libro XI* of the Code of Criminal Procedure will be applicable (arts. 969-*bis* ff. CPP).

When cooperation is requested by non-EU countries, bilateral or multilateral conventions will be applied. It is only in the absence of any conventions between Italy and the non-EU State that arts. 696-*bis* ff. CPP come into consideration.

Art. 30 of the Directive 2014/41/EU on EIO allows the interception of telecommunications with the technical assistance of another State, while subsequent art. 31 governs situations when there is no need of technical assistance. We must examine the operative provisions of *decreto legislativo* no. 108 of 2017, when the Italian judicial authority requests that another Member State makes an interception. Art. 43 of the *decreto* lays out the conditions and procedure for the Italian prosecutor to ask a foreign judicial authority for an interception. Art. 36 generally governs the admissibility in Italian trials of the "activities realised and evidence obtained in another country:" this provision is therefore applicable also to the results of interceptions. According to this article, authorities must insert in the trial dossier *(fascicolo per il dibattimento)*, provided in art. 431 CPP:

a) the documents obtained abroad through the EIO and the records of the one-off activities obtained in the same way;

b) the records of activities not included at letter a), obtained abroad through EIO when the defence counsels had the chance to attend and to exercise the powers recognised by Italian law.

There is no doubt that interceptions fall within the one-off activities provided in letter a).

Outside the recent EIO regime, interceptions legitimately authorised abroad are likely to be admissible in national trials. Indeed, art. 431 CPP allows the submission in the trial dossier of:

d) documents obtained abroad through letters rogatory and the records of one-off activities obtained in the same way;

(…)

f) the records of other acts not included at letter d) obtained abroad through letters rogatory when the defence counsels had the chance to attend and to exercise the powers recognised by the Italian law.

Moreover, art. 78 disp. att. CPP, entitled "acquisizione di atti di un procedimento penale straniero" (submission of acts of a foreign criminal proceeding) states:

1. The documents related to activities of a criminal proceedings of a foreign judicial authority can be submitted according to art. 238 CPP.

2. The one-time acts of the foreign judicial police can be filed in the trial dossier *(fascicolo per il dibattimento)* with the consent of the parties or after the testimony of the authors of the acts also through letters rogatory according to the adversarial principles.

Therefore, the jurisprudence supports the submission in criminal proceedings of interceptions made abroad with two limitations: the respect of the foreign criminal procedure and the conformity of that procedure with Italian fundamental principles.[37]

The jurisprudence has also raised the possibility of using foreign interceptions outside of the trial where the request for judicial assistance or the letters rogatory were requested.[38]

---

[37] See Cassazione penale, sezione II, 22-12-2016, Crupi, n. 2173, in CED, rv. 269000: "with regard to letters rogatory, the procedural provisions of the State where the act is realised are applicable, with the only limit that the evidence cannot be obtained in violation of the fundamental principles of the Italian judicial system and the rights of the defence" (in this case the Court rejected the defensive argument according to which the audio surveillance authorised by the Dutch authority should have been considered inadmissible, as the Dutch interception regime is consistent with the Italian principles protected by art. 15 Constitution); see also Cassazione penale, sez. I, 06/07/1998, n. 4048, in Banca Dati DeJure (on interceptions authorised by the German judicial authority).

[38] See Cassazione penale, sezione II, 13-12-2016, Commisso, n. 1926, in CED, rv. 268760: "with regard to interceptions realised within a foreigner criminal proceeding and submitted through letters rogatory, art. 8, para. 3 of the Protocol to the European Convention on mutual assistance in criminal matters, signed on 16 October 2001 and entered into force on 5 October 2005, repealed art. 50, para. 3 of the Convention implementing the Schengen Agreement of 19 June 1990. Thanks to this, the State Parties to the Convention are no more limited in using the transmitted documents in trials others than the one were the request for judicial assistance or the letters rogatory were requested;" this decision is

Ultimately, the jurisprudence has also clarified that foreign police activities are presumed legitimate and legal and only the judicial authority of that country can object to this presumption.[39]

4. Challenging the probity of intercepted data

In the analysis of the probity of intercepted data, two aspects deserve to be examined: on one side the content of the interceptions itself, on the other side the procedure to be followed when conducting interceptive operations.

With regards to the first aspect there are only few things to say. The jurisprudence notes that the interpretation and assessment of the conversations is a matter of fact and the judge of the fact is the only competent authority to decide on it. The *Court of Cassazione* can only and eventually rule on a manifest lack of logic and irrationality of the reasoning of the decision. The principle of independent evaluation of the evidence also concerns technical evidence, therefore the judge, the *peritus peritorum*, may not follow the assessment of the expert who transcribed the information in light of their perception of the audio files reproducing the content of the interceptions. With regard to the identification of the people involved in the intercepted conversation, the judge may rely on the declarations of police officers and agents who recognise the voices of the accused or on any other identifying element. The burden to prove that these declarations are wrong falls on the party challenging them.

The second aspect has already been broadly addressed. Arts. 267 ff. CPP describe in detail the procedure to be applied to interceptions. The infringement of the most important procedural rules results in inadmissibility of the evidence: see, for example, art. 271 para. 1 CPP. The defendant who wants the content of interceptions to be declared inadmissible must prove a violation of these provisions. There has been a lot of jurisprudence on this issue since 1989 (when the code entered into force) also of the *Sezioni Unite* (the plenary sessions of the *Corte di Cassazione*) and on multiple occasions complex interceptive operations were subject to the exclusionary rule.

---

consistent with Cassazione penale, sezione V, 18-05-2016,n. 26885, Commisso, in CED, rv. 267265.

[39] See Cassazione penale, sezione V, 16-11-2016, Ruso, n.1405, in CED, rv. 269015: "the use of investigative acts realised abroad by the foreigner police in order to ascertain the existence of the serious evidence of culpability *(gravi indizi di colpevolezza)* for the adoption of preventive measures is not bound to the ascertainment by the Italian judge of the legitimacy of the activity of the foreigner police, because there is a presumption of legitimacy of its activity and only the competent foreigner judicial authority can possibly question them" (the Court rejected the request for transmission of the original authorisations and records of interceptions made by the Dutch authority after the transmission to the Italian authority through letters rogatory).

For example, many judgments are related to the use of interceptive devices not available to the *Procura della Repubblica* but available to the judicial police or to private entities. The problem is related to the reasoning of the exceptional order deciding to delegate the activities to the judicial police or to the entity, because the insufficiency of the reasoning causes the inadmissibility of the evidence.[40]

On a technical level, it must be remembered that, when the *captatore informatico* is available for use, therefore not before 31 March 2019,[41] art. 7 of the *decreto legislativo* no. 216 of 2017 heading *Disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all' archivio informatico* will be applicable:

1. The technical requirements of the cyber-programs for interceptions through the captatore informatico on an electronic device are decided with decree of the Minister of justice to be issued within thirty days from the entry into force of this decree.
2. The technical requirements are established according to reliability, security and efficiency measures in order to assure that the cyber-programs can be used only to carry out the authorised operations.

The provision reveals the awareness of the legislator of the importance of the technical aspects of this delicate issue. Obviously, there is no direct link between the technical requirements and inadmissibility, but it will be interesting to follow the trials and the jurisprudence going forward.

---

[40] For example, see Cassazione penale, sezione I, 30-03-2016, Bettera, n. 36307, in CED, rv. 268112: "with regard to interception of communications and conversations, the reasoning of the urgent authorisation order of the prosecutor on the exceptional urgency justifying the use of devices available to the judicial police according to art. 268, para. 3 CPP does not include the technical aspects determining the functional suitability of the devices available at the Procura della Repubblica, whose omission makes null and void the order and determines the inadmissibility of the intercepted conversations." The Court clarified that the validating order of the pre-trial judge *(giudice per le indagini preliminari)* does not solve the vices of the prosecutor's order, because the lack of reasoning on the suitability of the devices available at the *Procura della Repubblica* is a condition imposed by law and relevant while the interception is ongoing.

[41] As we have seen, the captatore has already been – and possibly is still being – used in criminal investigations, despite the lack of governance. Therefore, we only mean that after 31 March 2019 the legal basis contained in the *decreto legislativo* no. 216 of 2017 will be applicable (see art. 9 of the *decreto*).

V. Exchange of Intercepted Electronic Communications Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

1. International conventions

The current normative sources system in the international judicial cooperation sector has already been outlined (see above, IV.3.c.).

Italy has implemented Directive 2014/41/UE of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters with *decreto legislativo* no. 108 of 21 June 2017. Arts. 30 and 31 of the Directive deal with interceptions. They correspond to arts. 23, 24 and 25 of the *decreto legislativo* no. 108 of 2017 dealing with the passive procedure (i.e., when a foreign State asks Italy to intercept) and arts. 43, 44 and 45 of the *decreto* dealing with the active procedure (i.e., when Italy asks a foreign State to intercept).

Recently, Italy ratified and executed, with *legge* no. 149 of 21 July 2016, the Convention on mutual assistance in criminal matters between the Member States of the European Union, signed in Brussels on 29 May 2000. This *legge* is crucial because, alongside ratifying the Convention (art. 1 and 2), it mandates the Government to implement the Convention itself (art. 3) and to completely reform *Libro XI* of the Code of Criminal Procedure (art. 4; *Libro XI* is dedicated to judicial cooperation with foreign authorities), and amends itself some parts of *Libro XI* (art. 5). Art. 3 of *legge* no. 149 of 2016 was implemented by *decreto legislativo* no. 52 of 5 April 2017 ("Implementation norms of the Convention on mutual assistance in criminal matters between the Member States of the European Union, signed in Brussels on 29 May 2000"). According to art. 27 of *decreto legislativo* no. 52 of 2017, the Convention entered into force for Italy on 22 February 2018. It goes without saying that the application of EIO will be default for the Member States of the European Union; nevertheless, the Brussels Convention will continue to be applied. As far as the scope of the Convention is concerned, it will be applied to cooperation acts which do not fall under the scope of application of EIO (such as notifications of acts, spontaneous information exchange, etc.).[42] With regard to the subjects, it will be applied to judicial cooperation with EU States which are not bound by EIO, such as Ireland and Denmark (see "whereas" no. 44 and 45 of Directive 2014/41/EU) and with some non-EU States that have negotiated the appli-

[42] A complete list of these activities, excluded from EIO and still in the scope of application of the 2000 Convention, is included in the Circular letter on the implementation of Directive 2014/41/EU on the European Investigation Order – operational manual, 2016/2017 of the Ministry for Justice, available on the website of the Ministry.

cation of specific norms of the Convention, such as Iceland or Norway.[43] The delegation contained in art. 4 of *legge* no. 149 of 2016 for the amendment of *Libro XI* of the Code of Criminal Procedure was exercised through *decreto legislativo* n. 149 of 3 October 2017.

In the past, Italy has also ratified:

– the European Convention on mutual assistance in criminal matters of 20 April 1956, with *legge* no. 215 of 23 February 1961, "Ratification and implementation of the European Convention on mutual assistance in criminal matters, signed in Strasbourg on 20 April 1959."
– the Convention on the application of the Schengen Agreements of 19 June 1990, with *legge* no. 388 of 30 September 1993.

Italy has also ratified the famous Budapest Convention on Cybercrime of 23 November 2001 of the Council of Europe with *legge* no. 48 of 18 March 2008. This piece of legislation not only authorised the ratification of the Convention, but it also introduced many amendments to the Criminal Code and the Code of Criminal Procedure (in this report amendments to inspections, search and seizure regime have been often quoted), in order to make the national legal order comply with the Convention. Without considering the matter in depth, it is worth noting that the aim was not completely fulfilled: some aspects of the Convention have not been implemented adequately.

Finally, Italy has also implemented the Convention and the Protocols of the United Nations against transnational organised crime, adopted by the General Assembly on 15 November 2000 and 31 May 2001, with *legge* no. 146 of 16 March 2006. This piece of legislation, as we observed dealing with IT crimes, not only authorised the ratification, but also modified the national legal order. Thus, no specific provision has been added in order to better implement art. 18 of the Convention, which includes various and complex rules on mutual judicial cooperation.

2. Bilateral treaties

It is difficult to illustrate the content of all bilateral treaties concluded by Italy to implement the Conventions listed in the previous paragraph – and those not stemming from them.[44]

---

[43] See the Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the application of some dispositions of the Convention of 29 May 2000 on mutual assistance in criminal matters between the Member States of the European Union and its Protocol of 2001.

[44] Therefore, it is useful to refer to the website of the Ministry for Justice, which shows a precise and updated (to 25 September 2017) list of these bilateral treaties, which can be filtered by theme or by country: https://www.giustizia.it/giustizia/it/mg_1_3.page.

As far as Germany is concerned, to give an example, only two bilateral agreements are quoted, both going back to 1979 and directed to facilitate the application of the extradition and judicial cooperation agreements in force at the time:

– Additional agreement to the European Convention on mutual assistance in criminal matters of 20 April 1959 and facilitating its application;
– Additional agreement to the European Convention on extradition of 13 December 1957 and AIMED AT facilitating its application (Rome, 1979).

Also because of the year of stipulation, the additional agreement on mutual assistance has no specific provisions on interceptions.

3. National regulation

As stated above, national legislation on judicial cooperation is included in *Libro XI* of the code of criminal procedure, and in the source hierarchy it is placed on the lowest level: pursuant to art. 696 CPP, it applies only if EU law, general international law or applicable international conventions in force make no provisions about the issue. A recent and minor exception concerns arts. 696-*bis* to 696-*decies* CPP, introduced by *decreto legislativo* no. 149 of 2017: these nine provisions establish generally applicable principles in EU competence matters (mutual recognition, third persons rights protection, etc.).

Furthermore, the norms of *Libro XI* are organised as follows: arts. 697–722 CPP deal with extradition, both to foreign countries (so-called passive extradition) and from foreign countries (so-called active extradition); arts. 723–729-*quinquies* CPP deal with letters rogatory (or judicial cooperation requests), divided into letters (or judicial cooperation requests) from foreign countries and to foreign countries; arts. 730-746 CPP deal with the effects of criminal judgments, both of foreign judgments in Italy and of Italian judgments in foreign countries.

None of these provisions expressly mention the interception of data or conversations, therefore general norms on letters rogatory (or judicial cooperation) will be applicable to them.

Beyond legal provisions, and specifically those regarding interceptions, the Italian jurisprudence on the so-called “istradamento” is relevant. From a technical point of view, *istradamento* is a mechanism used by the judicial authority and the police in order to avoid a formal letter rogatory, in the case of audio or telephonic surveillance.

As far as audio surveillance is concerned, it has been recently stated that: “the audio surveillance of conversations taking place partially abroad is fully legitimate, as long as recording procedures and verbalisation are carried out within the Italian territory, after the placement of wires and other devices to the up taking of conversations on vehicles in Italy. The forwarding of recorded conversations to the office

of the *Procura della Repubblica* can be carried out technically both with the *istradamento* on network and bridges of an Italian provider, and using the internet, without the need for an international letter rogatory. This is possible if the recording and verbalisation of conversations is carried out with the devices available at the *Procura della Repubblica* (apart from express derogations) and if these registrations with audio or IT content are kept by the *Pubblico Ministero.* Alternatively, the transfer to foreign territories successive to the start of surveillance would cause the technical impossibility to intercept, as the judicial authority could ignore the exact location of the vehicle, and therefore be hindered in asking for a letter rogatory, with neither the urgency nor methods provided for by art. 727, comma 5 CPP."[45]

As far as telephone tapping is concerned, it has been similarly stated that: "the usage of the *istradamento* technique, i.e., the collecting through a national provider of calls coming from a foreign country and directed to an Italian user, or vice versa, is fully legitimate and does not cause the violation of norms on international letter rogatories, since the whole interception, receiving and recording procedure of calls, is carried out in the State's territory."[46]

According to scholars, this clear case law must now be revised, as a consequence of the entry into force of EIO.[47]

B. Requirements and Procedure (Including the Handling of Privileged Information)

1. Incoming requests

The interception request coming from abroad is handled differently, depending on the legal basis on which it is rooted.

In the EIO system, the relevant norms are arts. 30 and 31 of the Directive 2014/41/EU, which deal with interceptions without distinguishing between incoming and outgoing requests, and arts. 23–25 of *decreto legislativo* n. 108 of 2017, which specifically handle the requests of the EU Member States to Italy. Art. 23 of *decreto legislativo* no. 108 of 2017 describes the procedure when Italian technical cooperation is necessary: the EIO is recognised by the *Procuratore della Repubblica* of the Tribunal of the district in which these acts must be carried out. Subsequently, the *Procuratore* forwards the request to the judge for preliminary investigation *(giudice per le indagini preliminari)* in order to be authorised; the interception can be carried out with immediate submission of data or with post-

---

[45] See Cassazione penale, sezione I, 23-03-2018, n. 35212, in Banca Dati DeJure.

[46] See Cassazione penale, sezione II, 04-11-2016, n. 51034, in Banca Dati DeJure.

[47] See *Ubertis*, Cassazione penale, p. 53.

poned submission. Art. 24 of *decreto legislativo* no. 108 of 2017 provides for cases where technical cooperation is not necessary: the foreign State in this case notifies the *Procuratore della Repubblica* of the beginning of the operations; the latter immediately informs the judge for preliminary investigation, who can order the ceasing of operations if the criminal offence in question does not provide for the possibility of interceptions in Italy. Finally, art. 25 of *decreto legislativo* no. 108 of 2017 governs data retention. It must be said that every investigation operation, including interceptions, should be simplified by using a single facsimile request form by the requesting authorities, attached to Directive 2014/41/EU. This form, once fully operational, should facilitate the establishing of common practices. For the person involved in interceptions no specific guarantees are provided; the general provision in question is therefore art. 13 of *decreto legislativo* no. 108 of 2017 entitled "remedies," according to which the person under investigation and his/her defence counsel can oppose the order recognising EIO before the judge for preliminary investigation within five days of its notification.[48]

If the Convention on mutual assistance in criminal matters between EU Member States, signed in Brussels on 29 May 2000, is applicable, the norms in question can be found in arts. 17–22, without distinction between incoming and outgoing requests. The *decreto legislativo* no. 52 of 5 April 2017, which incorporates the Convention into the Italian legal order, introduces arts. 19–21 without any distinction between requests coming from or going abroad. Thus, it provides a similar regulation to that of the EIO (except for the norms on remedies). The European Convention on mutual assistance in criminal matters of 20 April 1956, due to its date of inception, does not include specific provisions regarding interceptions.

Finally, no specific norm on how to deal with interception requests coming from abroad is included in the *Libro XI* of the Code of Criminal Procedure.

Two questions can therefore be raised: whether the Italian judicial authorities could subordinate the submission of data to limitations or conditions; and whether, in the submission of intercepted data, the Italian judicial authorities could somehow secure the respect of national provisions on privileges and secrets (para. III.B.3.), and, more generally, the system of interdiction to the use of interceptions, both of which have been examined above.

The first question evokes a difficult issue. The evidence procedure is complex: evidence is *admitted* at first; then it is *obtained*; in the end it is *evaluated*. Most of the problems caused by judicial cooperation in evidence procedures come from the fact that, in these cases, it is a State (the issuing State) which *admits* and *evaluates* evidence; but it is a different State (the issued State) that *obtains* it. We are confronted by the dilemma between *lex fori* and *lex loci*: in order to grant the full

[48] Please consider that even the Directive 2014/41/EU includes art. 14, entitled in fact "legal remedies."

availability of evidence, the issuing State has an interest in admitting, obtaining, and using the evidence according to one single piece of legislation (its own), i.e., the *lex fori*; but this is not always the case, because evidence is then obtained in the territory of a State which requires compliance with its own regulation (i.e., *lex loci*). Therefore, usually it is not the issued State which limits or conditions the use of evidence for the issuing States, but it is the issuing State which requires the issued State to comply with certain rules in the acquisition of evidence.

In the European Union the limitation of the use of evidence in one State, imposed by another State, on evidence acquired in its territory, could violate the principle of the freedom of movement and the principle of mutual recognition. Thus, in the EIO system preference is given to a "*consensus* principle:" when a State needs judicial cooperation from another, Directive 2014/41/EU provides for a mutually satisfactory agreement on the forms of acquisition. Art. 9 of Directive 2014/41/EU states that "the executing authority shall recognise an EIO […] without any further formality being required" (para. 1); that "the executing authority shall comply with the formalities and procedures expressly indicated by the issuing authority unless otherwise provided in this Directive and provided that such formalities and procedures are not contrary to the fundamental principles of law of the executing State" (para. 2); and that, in general, "the issuing authority and executing authority may consult each other, by any appropriate means, with a view to facilitating the efficient application of this Article" (para. 6). This "*consensus* principle" is enshrined in art. 4 co. 2 and art. 9 of *decreto legislativo* no. 108 of 2017 at the national level, which compels Italy to proceed with judicial cooperation requests coming from abroad, while complying with prescribed forms, and making adaptation or refusal of evidence only an exception.

Taking into consideration the very intrusive nature of interceptions, however, art. 23 of *decreto legislativo* no. 108 of 2017 states that the interception issued from a foreign State can be refused if "the admissibility requirements provided by the national legal order" are not fulfilled.[49] Moreover, all executive operations will be carried out with the timing foreseen by Italian law.

The Convention on mutual cooperation in criminal matters between the Member States of the European Union of 29 May 2000 follows the abovementioned principles. In art. 4 para. 1 it states: "where mutual assistance is afforded, the issued Member State shall comply with the formalities and procedures expressly indicated by the requesting Member State, unless otherwise provided in this Convention and

[49] This is not completely in contrast with the principle of mutual recognition, but is on the contrary in compliance with a very important principle for Directive 2014/41/EU, i.e., the principle that enables the State of execution to deny the cooperation request if the issued type of operation is not foreseen in its national law for a similar national case (whereas, no. 10).

provided that such formalities and procedures are not contrary to the fundamental principles of law in the issued Member State."

Additionally, art. 725, co. 1 CPP states that "for the handling of the requested operations, the dispositions of this code must be applied, saving the compliance with the special modalities expressly demanded by the foreign judicial authority, which must not be contrary to the principles of the national legal order."

As far as the second question is concerned, i.e., if in submitting the intercepted data the national legal order assures compliance with the abovementioned (III.B.3.) national law on privileges and secrets and, in general, with the system of interdiction of use of interceptions, there is no norm at the EU, international or national level which examines the problem. There is neither case law nor common practice on the issue. It is clear that if during surveillance operations the Italian police realise that they acted in violation of a privilege or a secret (for example, the police realise they are intercepting the person under investigation's conversation with their defence counsel), this would make the privilege or secret protection mechanisms operative exactly as it would in national cases. This reaction could be more difficult if the foreign State issued and obtained the immediate submission of communication flows; in these cases, in order to ensure compliance with the national provisions on secrets, it could be useful to create a norm that enables the State to limit the use of submitted data, as suggested in the questionnaire.

2. Outgoing requests

The reverse situation will now be addressed.

In Directive 2014/41/UE, as it does not distinguish between incoming and outgoing requests, the relevant provisions are the same ones analysed above, i.e., arts. 30 and 31. The *decreto legislativo* no. 108 of 2017, instead, dedicates arts. 43–45 to the interceptions requested by Italy to another EU Member State. Among other things, it states that the prosecutor issues the request for assistance to the foreign authority and it is their duty to specify whether they request the immediate or postponed transmission of communications. The Italian regime does not actually include the possibility for the prosecutor to request specific interceptions procedures to be observed; eventually, art. 33 of *decreto legislativo* no. 108 of 2017 could give the prosecutor this power, stating that "the judicial authority issuing the order agrees with the executing authority the procedure for the execution of the activity […]" (para. 1).

The same applies to the Convention on mutual assistance in criminal matters between EU Member States signed in Brussels on 29 May 2000: in this case, too, the relevant provisions (arts. 17–22) do not distinguish between incoming and outgoing requests. The *decreto legislativo* no. 52 of 5 April 2017, implementing the Conven-

tion on a national level, includes two provisions on the outgoing requests, arts. 22 and 23, placing on the prosecutor the burden to send the request abroad.

The *Libro XI* of the Code of Criminal Procedure, despite the fact that it does not include provisions on interceptions, contains two interesting provisions. The first one is art. 728 para. 9 CPP stating that "when, according to international treaties, the request for judicial assistance may be executed in line with the national procedure, the judicial authority indicates to the foreign authority the procedures and the other requirements to be observed in order to ensure the admissibility of the acts." The second one is art. 729 para. 1 CPP: "when the executing State imposes conditions on the use of the requested acts, the judicial authority is bound by these conditions." Both provisions describe two equivalent and reversed situations: when Italy requires the executing State to follow a specific procedure and when the executing State binds or limits the use of the act.

As for the incoming requests, the problem of the casual (or not) interception of secret conversations is not expressly regulated. On the contrary, as already seen, generally in Italy there is a presumption of legitimacy for the activities executed by a third country under requests for assistance or letters rogatory.[50] Nevertheless it is not an irrebuttable presumption:[51] in light of the complexity of the evidentiary system, including admission, submission and assessment, it is not groundless to say that as the evidence must be used in Italy, some criteria for the assessment of the evidence (the "Beweisverbote") must be used even if it is collected abroad. This is true in particular when these criteria protect primary interests, such as for the secrets regime (see above, para. III.B.3.).

3. Technical regulation

This aspect has already been discussed above at paras. 1 and 2.

4. Real-time transfer of communications data

The real-time transfer of communications data has both negative and positive sides to it. Among the positives, there is the general efficiency in responding to the request for assistance and the minimal organisational effort for the required State that, whenever possible, is only the intermediary between the requesting authority and the "source of evidence."

On the contrary, it is clear from the previous paragraphs that a disadvantage is the complete lack of control over the content of interceptions from the requested,

---

[50] See above, footnote no. 37.

[51] The limit imposed by the jurisprudence is the respect for fundamental rights (see above, footnote no. 37).

territorially competent State. This lack of control could be accepted, in theory, in light of the principle of mutual recognition and trust, if some sort of effective – yet sometimes difficult[52] – control would be granted by the requesting State when using the sent evidence.[53]

Apart from these general aspects, the immediate submission of intercepted data is already regulated at the EIO level: according to art. 30 para. 6 lit. a) every Member State can request another State to carry out the interception "transmitting telecommunications immediately to the issuing State;" the modules attached to the Directive should be taken into consideration (in particular Attachment A, section H7).[54] Italy has duly transposed this possibility in its implementation law: see art. 23, co. 4, lit. a) of decreto legislativo no. 108 of 2017.

It should be kept in mind that, before the EIO system, the possibility to immediately submit interceptions had already been foreseen by the Convention on mutual cooperation in criminal matters between the Member States of the European Union of 29 May 2000: art. 18 para. 1 lists the two alternatives, consisting of "the interception and immediate transmission to the requesting Member State of telecommunications" (lit. a) or of "the interception, recording and subsequent transmission to the requesting Member State of the recording of telecommunications" (lit. b). In this respect, see arts. 19 ff. of *decreto legislativo* no. 52 of 2017, which incorporates the 2000 Convention into Italian law.

Nevertheless, a direct dialogue between foreign authorities and an Italian telecommunications service provider does not seem possible yet: the filter of the Italian judicial authority is always necessary and – maybe – appropriate.

From the perspective of increasing the system's effectiveness, without damaging the individual's guarantees, the following considerations for the Italian legal order shall be underlined. For once, maybe, the above illustrated normative framework seems to be adequate or, at least, not in need of further immediate corrective interventions; yet, it is also necessary to monitor the effective use of the measure of immediate submission in terms of statistical consistency, and the common practices developing in this framework, especially between certain pairs of Member States; it

---

[52] What should be granted is the respect of technical provisions governing the deadlines, the procedure, and the means used for the interceptions. There are two alternatives: either the foreign judge applies the Italian provisions, or the Italian authority follows the foreign provisions. This problem could be easily avoided if common standards were approved at least within the EU, but it seems an objective far from being achieved.

[53] Such effective control would overcome the jurisprudence, like the Italian one, presuming the legitimacy of the acts executed by the foreign judicial authority on its own territory.

[54] Art. 28 of the Directive foresees the possibility to request, through EIO, investigative measures implying the gathering of evidence in real time, continuously and over a certain period of time.

is also necessary to identify the most frequent practical issues, in order to solve them through guidelines or good practices rather than through new legislation.

C. European Investigation Order

As widely anticipated, the EIO, introduced with Directive 2014/41/EU, aims to replace most of the instruments provided by the framework decisions and conventions.[55] It could become the most used MLA tool in the relationships between EU Member States, with an obvious growth of efficiency and ease in solving doubts and practical problems.

The *decreto legislativo* no. 108 of 2017 faithfully (or slavishly) transposed the directive and no additional or specific provisions were introduced with regard to interceptions (see above, paras. V.A. and V.B.).

D. Statistics

Starting from the premise that there is no specific statistic on transnational interceptions we can nevertheless provide a broad framework.

In Italy, among the judicial costs, item no. 1363 is dedicated to interceptions. In the framework of the spending review (art. 37 para. 16 of the *decreto-legge* no. 98 of 2011, signed into law with amendments by *legge* no. 111 of 15 July 2011) since 2012 each year before June the Minister of Justice presents the two Chambers of the Parliament with a report on the costs of justice. Since 2012 there have therefore existed some statistics on judicial costs in Italy.

Italy lacks, however, an internal organisation to conduct quantitative technical analysis of interceptions and there is no national authority with executive and control powers both for the judicial authority and the telecommunications operators. There is therefore no one supervising the whole operation at a national level. Italy merely relies upon the applicability of the Code of Criminal Procedure and the useful indication of the Authority for data protection. In Europe, Italy is renowned for having a high number of legitimately authorised interceptions. It is surprising to note that even if a relevant part of the investigative activities are grounded on interceptions, Italy – conversely to most of the other European Countries – does not possess a clear technical definition of this activity.

The Code for Cyber-Communications (*decreto legislativo* no. 259 of 1 August 2003) already included a "directory" *(repertorio)* that should have established a regulatory framework for the technical execution of interceptions, the specific du-

[55] With the exclusion of some specific activities, see above, footnote no. 42.

ties and the time limits. This "directory" would have harmonised the internal market, criticised by the EU Commission on 21 June 2012, who sent a letter of formal notice for the violation of Directive 2004/18/CE. The Commission criticised the complete lack of European public procedure for the purchase or rental of the interceptive devices of the *Procura*. This situation has also been described in the so-called *rapporto Giarda* (report), entitled "Elementi per una revisione della spesa pubblica" ("On the spending review"), presented to the Council of Ministers on 30 April 2012 by the Minister for the relationship with the Parliament. Facing an EU infringement procedure, the Minister of Justice issued a directive for the unique national call on interceptions. The website of the Ministry stated: "the unique call, without any consequence for the quantity and quality of interceptions, allows the saving of resources and gaining of personnel from the judicial offices, in addition to an improvement, including a technical one, of the quality of the service. The directive concludes the rationalisation of the matter thanks to a constant follow-up of these significant costs in conjunction with the saving of resources coming from the standard payment of telephonic operators." This directive, that still awaits implementation, included a technical attachment that would have replaced the directory established by the Code for Cyber-Communications and the prospect of the mandatory performances (see *Legge di stabilità*, *legge* no. 228 of 24 December 2012).

The *Direzione Generale di statistica e analisi organizzativa* (DG-Stat) was established within the Ministry of Justice through *Decreto del Presidente della Repubblica* in 2001. It is set at the *Dipartimento dell'organizzazione giudiziaria, del personale e dei servizi* (DOG) and it is part of the *Sistema Statistico Nazionale* (SISTAN). In order to implement the recent European directives on public statistics, the DG-Stat created a website (https://webstat.giustizia.it) dedicated to judicial statistics. Its activities include: the diffusion of the flows of information on civil law trials, organised into different Offices and macro-areas; follow-up on mediators' activities handled by the responsible authorities; following the performance of the judicial offices; and measuring the length of both civil and criminal proceedings.

With regards to the interceptions conducted in Italy, the *Direzione Generale di Statistica* started to collect statistics in 2003. The last report (2013–2015) highlights that:

– the number of targets increased by 82% in ten years, with an average annual rate of 6.2%. The information provided by some interceptive agencies shows that on average 1.6 targets per person are intercepted, that is to say that in 2013 about 90,000 people were intercepted;
– the increasing number included all types of interceptions by varying percentages: between 2003 and 2013 telephone targets increased by 82%, targets to be intercepted through audio surveillance increased by 62% and other targets, including cyber- and thematic interceptions tripled (202%). 2013 is the year with the highest number of targets;

– the percentage distribution of the targets, distinguished by type of interception, shows a clear prevalence for telephone tapping (89%) over audio surveillance (9%) and telematic (2%). Almost all of them are ordered during the investigations by the regular *Procura*, and one third of the targets are ordered by the *Direzioni Distrettuali Antimafia* (the office responsible for mafia-crimes investigations). The data on interceptions requested for anti-terrorism sections is marginal, though not insignificant. The territorial distribution of the intercepted targets in 2013 demonstrates that in the south of Italy and on the islands there is a larger use of audio surveillance, while in the centre and north telephone tapping is the most used kind of interception. There is no information on the effective duration of the interception, but thanks to the identification of a parameter determined in light of the number of authorisation orders and subsequent extensions, it has been possible to obtain the average duration. The overall duration of an average interception activity has been calculated on the weighted average of the duration of regular interceptions, whose time-limit fixed by law is 15 days with possible extensions of 15 days, and weighted average of the duration of the interceptions for organised crime (mafia crimes and terrorism), whose time-limit is 40 days, with possible extensions of 20 days. Moreover, as the target is a single device and each person may have more than one device, the average duration of the interception referring to the item "person under investigation" may be longer.

Bibliography

AA.VV., L'intercettazione di comunicazioni, a cura di Bene T. Cacucci, Bari 2018.

AA.VV., Le indagini atipiche, a cura di Scalfati A. Giappichelli, Torino 2014.

Agostini, Bianca, La disciplina delle intercettazioni preventive nel sistema antiterrorismo. Diritto penale contemporaneo, 2017, fasc. 1, pp. 141 et seq.

Barrocu, *Giovanni*, La cooperazione investigativa in ambito europeo – Da Eurojust all'ordine di indagine. Cedam, Padova 2017.

Basile, Fabio, Tassatività delle norme ricognitive della pericolosità nelle misure di prevenzione: Strasburgo chiama, Roma risponde, available at www.penalecontemporaneo.it [last visited March 2020].

– Quale futuro per le misure di prevenzione dopo le sentenze De Tommaso e Paternò? Giurisprudenza italiana, 2018, pp. 455 et seq.

Cupelli, Cristiano, La Corte costituzionale chiude il caso Taricco e apre a un diritto penale europeo 'certo'. Diritto penale contemporaneo, 2018, fasc. 6, pp. 227 et seq.

Flor, Roberto, Cyber-criminality: le fonti internazionali ed europee, in AA.VV., Cybercrime – Diritto e procedura penale dell'informatica. Utet Giuridica, Torino, pp. 97–139.

– Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad protection ai più recenti sviluppi. Diritto di Internet, 3, 2019, pp. 453–467.

Flor, Roberto, Riservatezza informatica e sicurezza informatica quali nuovi beni giuridici penalmente protetti, in AA.VV., Mobilità, sicurezza e nuove frontiere tecnologiche. Giappichelli, Torino 2018, pp. 463–482.

– Cyber-terrorismo e diritto penale in Italia, in Fornasari, Gabriele/Wenin, Roberto (eds), Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali. Trento-Napoli 2017, pp. 325–359.

– Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet, in Pérez Álvarez, Fernando (ed.), Serta in memoriam Louk Hulsman. Universidad de Salamanca, Salamanca (España) 2016, 329 et seq.

– Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo? Il diritto all'oblio su Internet dopo la sentenza Google Spain. Roma, Roma Tre-Press, 2015, 223 et seq.

– La Corte di Giustizia considera la Direttiva europea 2006/24 sulla c.d. data retention contraria ai diritti fondamentali. Una lunga storia a lieto fine? Diritto Penale Contemporaneo Rivista Trimestrale, 2014, 178 et seq.

– Nuove tecnologie e giustizia penale in Europa, tra le esigenze di accertamento e prevenzione dei reati e quelle di tutela della riservatezza: il ruolo "propulsore" della Corte di Giustizia, in Studi in onore di Maurizio Pedrazza Gorlero. Napoli, Edizioni Scientifiche Italiane 2014, 247 et seq.

– Perspective for new types of "technological investigation" and protection of fundamental rights in the Era of Internet. The so-called "cyberterrorism" as a prime example, between problems of definition and the fight against terrorism and cybercrime, in Delito, pena, politica criminal y tecnologìas de la informatiònen las modernascienciaspenales. Salamanca, Ediciones Universidad de Salamanca 2012, 51 et seq.

– Verso una rivalutazione dell'art. 615 ter c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nellera di Internet. Diritto Penale Contemporaneo Rivista Trimestrale, 2, 2012, 126 et seq.

– Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention. Ciberspazio e Diritto, 11, 2, 2010, 359 et seq.

– Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung. Rivista Trimestrale di Diritto Penale dell'Economia, 2009, 695 et seq.

Flor, Roberto/Falcinelli, Daniela/Marcolini, Stefano (eds.), La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet. DiPLaP Editor, Milano 2015.

La Rocca, E. Nadia, Intercettazioni, utilizzo di impianti esterni, instradamento: garanzie tecniche e prassi devianti. Giurisprudenza italiana, 2011, 731 et seq.

Manacorda, Stefano/Flor, Roberto/Joon, Oh (eds.), Cyber-criminality: Finding a balance between freedom and security. Milano 2012.

Marcolini, Stefano, Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta, in Cassazione penale, 2015, fasc. 2, pp. 760 et seq.

– L'istituto della data retention dopo la sentenza della Corte di Giustizia del 2014, in AA.VV., Cybercrime – Diritto e procedura penale dell'informatica. Utet Giuridica, Torino, pp. 1579–1597.

Marcolini, Stefano/Militello, Elena/Ruggieri, Francesca, Il caso Taricco e l'affermazione del principio di legalità processuale, in Bernardi, Alessandro/Cupelli Cristiano (eds.), Il caso Taricco e il dialogo tra le Corti. Jovene, Napoli 2017, pp. 223 et seq.

Picotti, Lorenzo (ed.), Tutela penale della persona e nuove tecnologie. Cedam, Padova 2013.

– Diritto penale e tecnologie informatiche: uno sguardo di insieme, in *AA.VV*., Cybercrime Diritto e procedura penale dell'informatica. Utet Giuridica, Torino, 2018, pp. 35–96.

– Aspectos penales del uso y el abuso de las redes sociales, in Derecho penal y nuevas tecnologìas. A proposito del Titulo VII bis del codigo penal. Universidad Sergio Arboleda, 2016, 255 et seq.

– Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico. Archivio penale, 2/2016, 354 et seq.

– Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l'informatique. RIDP, 2006, n. 3/4, 525 et seq.

– Il diritto penale dell'informatica nell'epoca di Internet. Cedam, Padova 2005.

Ruggieri, Francesca, Data retention e giudice di merito penale – Una discutibile pronuncia. Cassazione penale, 2017, 2483 et seq.

Signorato, Silvia, Le indagini digitali – Profili strutturali di una metamorfosi investigativa, Giappichelli, Torino 2018.

Tabasco, Giuseppe, Principio di proporzionalità e misure cautelari. Cedam, Padova 2017.

Torre M., Il captatore informatico – Nuove tecnologie investigative e rispetto delle regole processuali. Giuffrè, Milano 2017.

Trogu, Mauro, Sorveglianza e "perquisizioni" *on line* su materiale informatico, in Scalfati, Adolfo (ed.), Le indagini atipiche. Giappichelli, Torino 2014, pp. 431 et seq.

Ubertis, Giulio, Considerazioni generali su investigazioni e prove transnazionali. Cassazione penale, 2017, 49 et seq.

List of Abbreviations

AISE	Agenzia informazioni e sicurezza esterna
AISI	Agenzia informazioni e sicurezza interna
CISR	Comitato interministeriale per la sicurezza della Repubblica
CIT	centro intercettazioni telecomunicazioni
CJEU	Court of Justice of the European Union
CP	codice penale

CPP 1930	codice di procedura penale abrogato
CPP	codice di procedura penale
DIS	Dipartimento delle informazioni per la sicurezza
disp. att. CPP	norme di attuazione, di coordinamento e transitorie del codice di procedura penale
ECHR	European Convention on Human Rights
EIO	European Investigation Order in criminal matters
G.I.P.	giudice per le indagini preliminari
P.M.	pubblico ministero
RIDP	Revue Internationale de Droit Pénal

The Netherlands*

National Rapporteur:
Niels van Buiten

* This report reflects legislation and case law as of January 2019. I sincerely thank Prof. Dr. Bert-Jaap Koops and Mr. François Smulders for their contributions in reviewing Chapters I.–IV. and V., respectively.

Contents

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Security Services with Powers of Telecommunication Interception

1. National security architecture

In the Netherlands, several national services are equipped with powers regarding interception of electronic communications to assist them in their respective objectives. These institutions can generally be divided into intelligence and criminal investigation services and further subdivided based on their specific tasks.

a) Intelligence and Security Services

aa) Framework

The Dutch intelligence community consists of two agencies; the Military Intelligence and Security Service[1] (MIVD) and the General Intelligence and Security Service[2] (AIVD). As the names of the services suggest, they are both individually responsible for intelligence *and* security tasks within their respective fields of interest. The AIVD focuses on national security, where maintaining national security consists of several subtasks; investigating organisations and persons who might pose a risk, gathering intelligence on foreign entities and states, drawing up threat and risk analyses and providing security clearance, amongst others.[3] Where the AIVD is mainly focused on threats to Dutch society, the MIVD is more focused on peace operations and international terrorism. It gathers intelligence that is used in military operations and for the security of the Dutch military forces. As national and international security become more and more intertwined, the AIVD and MIVD are increasingly joining forces to avert risks and gather information.[4]

bb) Legal regime

Both Intelligence and Security Services (hereafter: ISS) are subject to the same legal framework, the Intelligence and Security Services Act 2017 (hereafter:

---

[1] Militaire Inlichtingen- en Veiligheidsdienst, MIVD.

[2] Algemene Inlichtingen- en Veiligheidsdienst, AIVD.

[3] The tasks are set out in article 8 of the Intelligence and Security Services Act 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017)).

[4] https://www.defensie.nl/organisatie/bestuursstaf/eenheden/mivd

ISSA),[5] which recently came into force. The framework has generally only been slightly altered compared to its predecessor, with the intention of aligning the legal framework with modern conditions. However, on specific topics and provisions the use of certain methods was either limited or expanded.[6]

An example of the latter is a newly added provision, article 48 ISSA, which permits the ISS not only to intercept the digital communications of a target and their associates, but also people in their vicinity (e.g., on their block or in their city) in the context of interception within a 'focused research assignment.'[7] An advisory referendum was held in light of the proposed Act, nicknamed 'the Dragnet-Act' due to this provision, which resulted in a no-vote-majority. However, after minor changes were made to specific provisions, the proposed Act nonetheless went into effect on 1 May 2018.

cc) Interception of electronic communication

The newly enacted legal framework of the ISSA provides the ISS with a specific provision on intercepting communications. Article 47 ISSA states that the services are competent 'to intercept, receive, record and listen in on any kind of conversation, telecommunication or data transfer via a 'computer system','[8] wherever it takes place, which they can do via technical means. Based on this provision, the services are also allowed to decrypt these conversations, telecommunications or data transfers. To use this measure in an operation, the director of either ISS has to submit a formal request to his respective Minister; either the Minister of the Interior for the AIVD or the Minister of Defence for the MIVD. Any request for the use of a special measure should contain an indication of the person or organisation with regard to whom the measure is requested, a description of the investigation for which the measure is to be deployed and with what purpose, and why it is necessary to do so.[9] Furthermore, for a formal request to intercept communications, the number or technical characteristics of the communications that are to be intercepted have to be provided if known. If the requirements are met, permission is granted and the requested special measure can be deployed for a maximum of three months. If the permission for intercepting communications was granted based on a request

---

5 Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017).

6 Explanatory Memorandum to the ISSA.

7 "Onderzoeksopdrachtgerichte interceptie;" this interception measure consists of three stages: (1) targeted acquisition of telecommunications, (2) pre-processing the intercepted telecommunications and (3) further processing the telecommunications, dealt with in articles 48, 49 and 50 ISSA respectively. As mass surveillance of communications does not fall within the scope of this report, it will not be dealt with in further detail.

8 Translation by the author of: 'geautomatiseerd werk,' which defines: "a device or a group of interconnected or coherent devices, of which one or more automatically process computer data using a software program."

9 Article 29 sub 2 ISSA.

that mentioned specific numbers or technical characteristics, other numbers or technical characteristics of the persons or organisations can also be intercepted when they become known after the permission is granted.[10]

dd) Cooperation with private parties

In order to intercept communications the Intelligence and Security Services can seek cooperation with communications networks and service providers, who are obliged to cooperate based on article 13.2 of the Telecommunications Act (hereafter: TA).[11] However, this provision only deals with *public* communications service providers. As the number of different kinds of communications service providers has grown exponentially over the last two decades and the possibility of discerning whether they are public has become more diffuse, in the explanatory memorandum of the ISSA the legislator expressed the need for a broader cooperation duty for these providers.[12] Therefore, specific provisions were introduced in the ISSA to ensure that the interception of communications and the performance of related measures can be achieved through obligatory cooperation from *any* communications services provider.[13]

b) Police Services

aa) Layout

The tasks of (reactive) criminal investigative and preventative policing are both performed by various police agencies in the Netherlands. The National Police is tasked with upholding the law and maintaining public order, but is also the main investigative organisation which assists the Public Prosecutors Office in fighting crime in general.

The Royal Military Police is a police force with military status, governed by the Ministry of Defence. Although officers of the Military Police have the same legal status as officers of the National Police and have the same competences towards civilians, their main tasks are policing activities abroad, maintaining border security and securing high risk targets, e.g., the Royal family, the Dutch National Bank and certain ministries.

While the officers of the National Police and the Military Police are competent to investigate and prevent criminal acts *in general*, there are also those working for one of the several special investigative services, such as the Fiscal Information and

---

[10] Article 47 sub 7 ISSA.

[11] See Appendix.

[12] Explanatory memorandum to the ISSA, s. 3.3.4.4.7.2.

[13] Articles 51 to 57 ISSA.

Investigation Service (FIOD).[14] These services have been designated to investigate criminal behaviour in specific fields; the FIOD, for instance, operates to counter fiscal, financial and economic fraud. In addition to the FIOD, there is the Inspectorate SZW (ISZW),[15] the Netherlands Food and Consumer Safety Authority (NVWA)[16] and the Human Environment and Transport Inspectorate (IL&T).[17] Although these organisations focus on certain specific acts of criminal behaviour, their toolkit for performing their respective investigations – e.g., the coercive powers and special investigative measures[18] they have at their disposal – does not differ greatly from those of the general investigative services like the National Police. This is especially the case since recent changes have been made to the DCCP and related legislative bodies, which mean that the special investigative services and Military Police are now independently competent to execute infiltration measures,[19] measures regarding systematic information gathering[20] and intercepting confidential communications.[21, 22] In effect, any inequality between the powers of investigative officers of different investigative services has been removed by the amendment.[23]

bb) Legal regime

Within the Dutch Code of Criminal Procedure[24] (hereafter: DCCP), a specific section[25] is dedicated to special investigative powers that can be used by all investigative officers mentioned above, which includes the interception of electronic communications. The framework governs all possible special investigative measures investigative officers can use to gather evidence in criminal investigations, as well as the limitations, thresholds and safeguards relevant to those actions. This part of the Code is split into three parts, all containing the same special investigative measures, but with different thresholds and limitations. The first chapter gov-

---

14 'Fiscale inlichtingen- & opsporingsdienst.'

15 'Inspectie Sociale Zaken & Werkgelegenheid:' focuses on labour market fraud, working conditions, etc.

16 'Nederlandse Voedsel- & Warenautoriteit:' guards the safety of food and consumer products, the welfare of animals and plants and upholds legislation on flora and fauna.

17 'Inspectie Leefomgeving & Transport:' supervisor in the field of safety, security and trust in transport, infrastructure, environment and living.

18 Such as intercepting electronic communications.

19 Article 126h DCCP.

20 Article 126j DCCP.

21 Article 126l DCCP.

22 Amendment Reinforcement of combatting organized crime, see Appendix.

23 NJB 2018; also Explanatory Memorandum to the Amendment.

24 Wetboek van Strafvordering.

25 Which was added to the DCCP after ratification of the Special Investigative Measures Act, the 'Wet op de Bijzondere Opsporingsbevoegdheden.'

erns reactive investigations and requires the reasonable suspicion that a crime has been committed. The second chapter oversees the use of special investigative measures in investigations where it is suspected that crimes that (would) seriously breach the rule of law, are being planned or committed in an organized context, e.g., criminal enterprises. This chapter provides, to some extent, the opportunity to take action preventatively, so that serious acts of criminal behaviour can be averted. The last chapter, relating to terrorist offences, oversees the use of special investigative measures in cases where a reasonable suspicion has not yet been established, but where there is a mere indication that an act of terrorism is being planned or committed; as the occurrence of terrorist acts is to be prevented at all cost, the level of suspicion required for the use of coercive and, especially, for the use of special investigative measures, is significantly lower compared to under the other two chapters.

cc) Interception of electronic communication

Based on article 126m DCCP the Police Services can use the special investigative measure of intercepting electronic communications in reactive criminal investigations. In case of investigations into crimes that are being planned or committed in an organized context, the services can use the provision of article 126t DCCP, and, in case of investigations into an indication that an act of terrorism is being planned or committed, use can be made of the provision of article 126zg DCCP. Although the texts of the provisions are fairly similar, the requirements and thresholds differ slightly between them. For the use of interception in a reactive investigation it has to be suspected that a crime mentioned in article 67 sub 1 DCCP has been committed. This provision mentions all the criminal acts for which suspects can be placed in pre-trial detention. Generally, this is for all criminal acts that are punishable with a maximum of at least four years imprisonment, but over the years several other crimes that do not meet that criterion have been added to the list. When a subject is suspected of having committed one of the criminal acts mentioned in article 67 paragraph 1 DCCP, an interception order can be requested based on article 126m DCCP.[26] The provision of article 126t DCCP can be used to acquire an interception order in both reactive and preventative investigations, but its use is restricted to subjects who are suspected of planning or committing criminal acts[27] in an organized context. Although partly worded differently, the other requirements in articles 126m and 126t DCCP do not differ significantly. The same applies to article 126zg DCCP; all requirements are fairly similar. The only significant difference is that an interception order can be acquired based on this provision

[26] Further requirements that have to be met for a request to be granted will be dealt with in section III.B.

[27] Again, criminal acts mentioned in article 67 para. 1 DCCP.

when there is (merely) an *indication* that a terrorist act – terrorist acts are exhaustively listed in article 83 Dutch Criminal Code – is being planned or committed.

dd) Cooperation with private parties

During the execution of the various special investigation orders and production orders, cooperation is often sought with private parties by the investigation authorities. To ensure that third parties cooperate in the execution, several special investigative measures are equipped with a codified cooperation duty, whereby breach of the duty can lead to criminal charges; several of these duties will be elaborated upon in section III.B. Duties on third parties regarding the use of interception measures that focus on electronic communications require these parties to cooperate once the formal and substantive prerequisites have been met and an official interception order has been established. The communications networks and services of public providers have to be interceptable[28] and these providers have to forward the intercepted communication that is requested to a specific unit of the National Police, tasked with the oversight of the execution of special investigative measures regarding interception: the Interception & Sensing[29] unit (hereafter: I&S, previously known as the Unit National Interception).[30, 31] This unit checks whether the investigative units have gathered all required official reports that are mandatory for the execution of interception measures[32] and is the hub between the authorities (National police, special police services and the Public Prosecutors office) and the providers. The information gathered is securely stored at the I&S, whose files can be remotely accessed by certain, certified officers within the various police units. These units generally have a specific 'taproom' at their disposal, from which the intercepted communications can be listened to – either live or afterwards.[33]

c) Legitimacy of data transfers between different security agencies

aa) Among Intelligence and Security Services

The Dutch Intelligence and Security Services, the AIVD and the MIVD, are obliged to work together as much as possible, according to article 86 sub 1 ISSA. This obligation entails both the duty to provide technical and other means of sup-

---

28 See section III.B.5.b.

29 'Interceptie & Sensing.'

30 'Unit Landelijke Interceptie,' or 'ULI'.

31 See: WODC 2012, s. 4.1.

32 Also when, in cases of emergency, an interception order is acquired verbally, in which case the official reports have to be acquired within three days. If not, the I&S will terminate the interception measure.

33 WODC 2012, s. 4.5.2.

port, as well as the duty to provide data. Article 88 ISSA deals with the cooperation with foreign Intelligence and Security Services; the Dutch Services are competent to enter into cooperative relationships with appropriate intelligence and security services from other countries. Whether or not other foreign services are appropriate to cooperate with and what the intensity and form of the cooperation should be, is dependent on:

1) the democratic embedding of the specific service in its country of origin,
2) the respect for human rights by the country concerned,
3) the professionalism and reliability of the specific service,
4) the legal powers and capabilities of the service in its country of origin, and
5) the level of data protection provided by the relevant service.[34]

If such a cooperative relationship is established, the Dutch Services are allowed to share information beneficial to the interests of their foreign counterparts, as long as these interests are compatible with the interests of the Dutch Services and the sharing of data will not negatively impact the performance of the Dutch Services.[35] In cases where there are urgent or important reasons to do so in the interest of the national ISS, the national ISS can provide information to foreign ISS even if there has not been established a cooperative relationship based on article 88 ISSA.[36]

bb) Between ISS and Police Services

Although the tasks of the Intelligence and Security Services and the Police Services differ, information can be and is exchanged between them. Articles 93 and 94 ISSA respectively oblige members of the Public Prosecutors Office and officers of the National Police, Military Police and National Tax Authority (which includes the FIOD) to report, via their superiors, any data that could be of interest to one of the ISS – either on request or voluntarily. The ISS can provide Ministers, governing bodies, people and organisations with processed data when it deems relevant.[37] When certain (processed) data[38] might be relevant for the detection and prosecution of criminal offences, the ISS can provide the Public Prosecutors Office with said data, either voluntarily or on request.[39]

---

34 Article 88 ISSA.

35 Article 89 ISSA; article 62 para. 1 under d ISSA.

36 Article 64 ISSA.

37 Article 62 ISSA.

38 Which can be the result of intercepted communication.

39 Article 66 ISSA; recordings of intercepted communications have been used in at least two criminal cases concerning terrorism: HR 05 September 2006, ECLI:NL:HR 2006: AV4122, *NJ* 2007, 336, m.nt. T.M. Schalken. However, such sharing by the ISS is *very* rare. Another case in which such sharing was performed: Hof Amsterdam 25 March 2014, ECLI:NL:GHAMS:2014:915.

cc) Among Police Services

In Dutch legislation several possibilities exist for sharing police data among Police Services, but for sharing the results of special investigative measures a special provision has been implemented. Article 126dd DCCP deals with information transfer from one investigation to another; the Public Prosecutor can decide[40] that data that was generated by the use of the special investigative measures of (1) observation using technical means, (2) the interception of confidential communication (eavesdropping), (3) production orders on data of a user and the telecommunications traffic data of that user and (4) the interception of telecommunications, can be used for an investigation other than the investigation for which the measures were originally used. Whether or not the other investigation runs within the same Police Service is irrelevant. For the transfer of interception results to a Police Service in another country the rules of mutual legal assistance apply, which will be dealt with in chapter V.

B. Statistics on Telecommunication Interception

1. Intelligence and Security Services

Although the Dutch Intelligence and Security Services are very secretive in nature and rarely seek publicity, in 2017 they made headlines twice – unintentionally. Alongside the controversy that arose around the proposal for the 'Dragnet'-Act,[41] a verdict by the Dutch Council of State caught the attention of the media. A Dutch foundation focusing on digital civil rights, Bits of Freedom, brought a case to the Council of State to move the AIVD to release statistics on its use of interception measures. The Minister of the Interior – to whom the AIVD is accountable and to which it reports[42] – had (for years) refused to do so, arguing that the release of these statistics might jeopardise national security. After the Council concluded that the Minister had given insufficient justification for his decision to not publicise the statistics,[43] the Minister chose to release the statistics for the years 2002 up to 2017 and also announced that new statistics would be published annually.[44]

---

40 Mostly on request by another public prosecutor.

41 See section I.A.1.a.bb.

42 Article 2 ISSA.

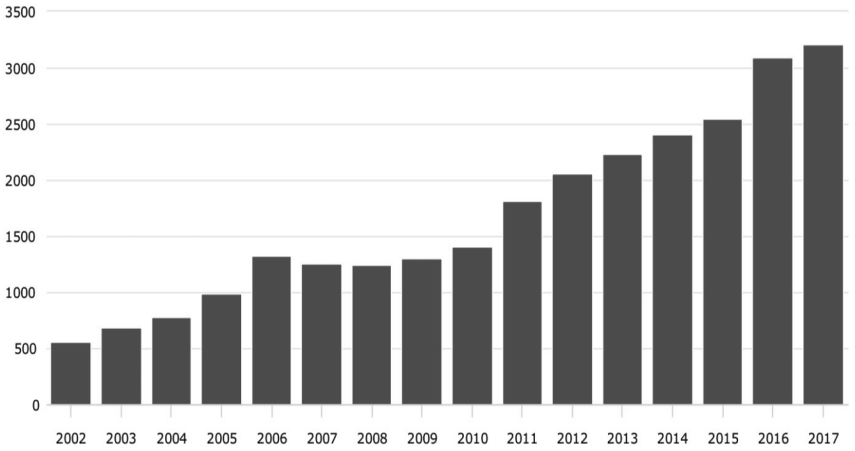
43 RvS 20 December 2017, ECLI:NL:RVS:2017:3508.

44 *Kamerstukken II* 2017/18, 29 924, nr. 154.

In the chart below[45] the number of individual taps on *devices* is given, that were deployed annually in the last two decades. These numbers therefore do not represent the number of targets that were investigated, as the communications of one subject can be intercepted on several devices and in several ways; the numbers include wiretaps, internet taps and the use of microphones. The steady rise of the number of deployments per year is explained by the changing communications landscape, as individuals tend to own more devices than they used to.[46]

For the Military Intelligence and Security Service, the counterpart of the AIVD, the statistics were also published after the verdict by the Council of State.[47] Again, as is the case for the chart published by the AIVD, the numbers in the chart below[48] reflect the use of interception on *devices*, not targets. Also, the numbers represent the use of wiretaps, internet taps and the use of microphones combined.

General Intelligence and Security Service – AIVD



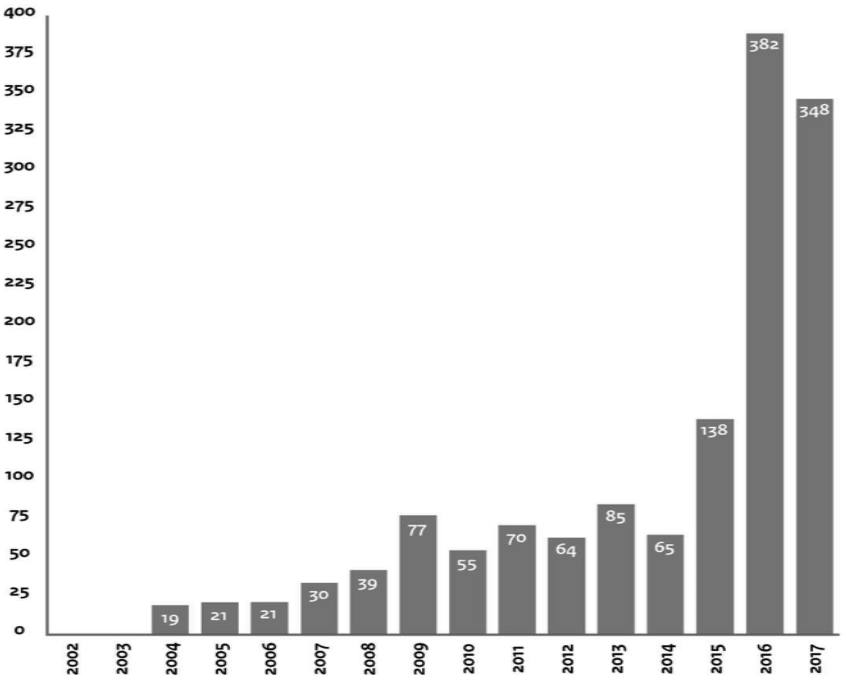
[45] Source: website of the AIVD, https://www.aivd.nl/onderwerpen/afluisteren/tapstatistieken

[46] https://www.aivd.nl/onderwerpen/afluisteren/tapstatistieken

[47] Although the MIVD was not part of the lawsuit, the Minister of Defence chose to treat the MIVD and AIVD equally, therefore releasing its statistics as well.

[48] Source: https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/tapstatistieken

Military Intelligence and Security Service – MIVD



2. Police Services

As mentioned in section I.A.1.c.dd., the interception of all Police Services is centralised at the I&S, which, as determined by the Minister of Justice and Security,[49] publishes its interception statistics in the annual reports on the performance of the Ministry of Justice & Security.

It should be noted that the numbers represent all the interception orders that were given in a specific year and from all police services combined, thus the interception quantities of mobile devices and landlines have been combined. The same goes for IP-taps, the figures for which constitute a combination of the amount of mail-taps *and* internet-taps that were deployed in a single year. Furthermore, as of 2014 a new interception standard was implemented, based on which there no longer is a technical or procedural difference between a phone and an internet tap. A differentiation in the respective numbers is therefore no longer made.[50] Extensions of inter-

[49] As of 2007, by ordered the (then) Minister of Justice; *Kamerstukken II* 2007/08, 30 517, nr. 6.

[50] *Kamerstukken II* 2016/17, 34 725-VI, nr. 1, p. 57.

ception orders are not included in the statistics, yet renewed authorizations for a number or IP-address that has been intercepted in the past *are* included.[51] The 'averages per day' reflect the total number of devices intercepted on average per day.[52]

Police Services[53]

	2010	2011	2012	2013	2014	2015	2016	2017
Numbers intercepted	22,006	24,718	25,487	26,150	25,181	24,063	24,850	24,900
Average per day	1,635	1,638	1,293	1,391	1,386	1,415	1,423	1,421
IP-taps	1,704	3,331	16,676	17,806	–	–	–	–
Average per day	131	339	727	829	–	–	–	–

Chart: produced by author.

II. Principles of Telecommunication Interception in Constitutional and Criminal Procedural Law

A. Constitutional Safeguards of Telecommunication

The use of special investigative measures based on the Dutch Code of Criminal Procedure involves various safeguards regarding privacy and other human rights principles. Yet, Koops points out that the Dutch Constitution (hereafter: DC) plays only a limited role in the legislation and legal practice of said criminal procedure, as the legislator focuses primarily on the European Convention on Human Rights for guidance on fundamental-rights protection.[54] Some constitutional protection surrounding communications data can however be found; article 10 DC represents the right to privacy and states that anyone shall have the right to respect for his privacy, which can only be infringed based on codified limitations. Article 10 DC also mandates that rules to protect privacy shall be laid down by Acts of Parliament regarding the recording and dissemination of personal data, and subsequently states that Acts of Parliament have to provide rules concerning the rights of persons to be informed of data recorded about them and the use that is made thereof, as well as to

---

51 WODC 2012, s. 5, 5.1 and 5.3.

52 Not the total of new interception orders granted each day.

53 Sources: *Kamerstukken II* 2010/11, 32 710-VI, nr. 1, p. 67 (referring to statistics provided by the National Unit of the National Police); *Kamerstukken II* 2016/17, 34 725-VI, nr. 1, p. 57 (referring to numbers provided by the National Unit – National Police); WODC 2012, pp. 82–83.

54 B.J. Koops, *Criminal investigation and privacy in Dutch law*, s. 2.2.1.

be able to have the data corrected.[55] Furthermore, article 13 DC protects the content of mediated communications via letters, telephone or telegraph, as a further elaboration on article 10 DC.[56] Article 13 paragraph 1 DC states that the privacy of correspondence (via letters) is inviolable, except in cases laid down by Acts of Parliament and by order of the court. Article 13 paragraph 2 DC complements this and states that the privacy of the telephone and telegraph is inviolable as well, except in cases laid down by Acts of Parliament and by or with the authorisation by those designated by an Act of Parliament.[57] As the mention of the telegraph already suggests, the DC is quite archaic: it has not been updated for decades and therefore is not reflective of the contemporary communications landscape. This results in electronic communications not being protected by the above provision (despite multiple attempts to correct this).[58] However, electronic communications data is largely treated equally to the other types of communication mentioned above, at least in lower legislation such as the DCCP. As for regular communications data, the constitutional protection only covers communications content, not traffic data.[59] As mentioned above, constitutional provisions and safeguards surrounding communications data are scarce; further provisions regarding (the protection of) communications data, such as the principle of proportionality, subsidiarity and necessity, are to be found in lower legislation and will be dealt with in section III.B.

B. Other, Non-Constitutional Legal Safeguards for Communications Data

Complementary to and based on the constitutional safeguards mentioned in the previous section, several provisions in other bodies of legislation protect data that is being or has been transmitted. These can be divided into provisions dealing with the protection of the secrecy of telecommunication, provisions on protecting personal computer stored data and provisions on special content transmitted by telecommunication.

1. Protective provisions in the Dutch Criminal Code

Multiple DCC provisions deal with breaches of the secrecy of communications, of which an overview is presented below:

---

55 Article 10 paras. 2 and 3 DC.

56 D.E. Bunschoten, *T&C Grondwet & Statuut*, article 13 Gw.

57 Constitution of the Kingdom of the Netherlands, official translation 2008, https://www.government.nl/documents/regulations/2012/10/18/the-constitution-of-the-kingdom-of-the-netherlands2008

58 D.E. Bunschoten, *T&C Grondwet & Statuut*, article 13 Gw, comment 6.

59 Koops 2016, s. 2.2.2.

Article 138ab DCC

The person who commits computer trespassing and (during which) unlawfully intercepts data (among other things), can be punished with up to 4 years imprisonment.

Article 139a DCC

He who secretly records a conversation in a house, private room or yard, other than with consent of a person partaking in said conversation, can be punished with up to 6 months imprisonment.

Article 139b DCC

He who secretly records a conversation other than in a house, private room or yard, without consent of a person partaking in said conversation, can be punished with up to 3 months imprisonment.

Article 139c DCC

The person unlawfully performing the interception or recording of a conversation that is not meant for that person and that is transmitted through the use of telecommunications or via a computer system, can be punished with up to 2 years imprisonment.

Article 139d DCC

He who places technical means in a place with the intention to listen in on, record or intercept a conversation, telecommunications, a data transfer or the data processing by a computer system, can be punished with up to two years imprisonment. Paragraph 2 of the provision states that a person is equally punishable, if he – with the intent that an act as described in article 138ab, paragraph 1, article 138b[60] or 139c DCC can be committed – 1) produces, sells, acquires, imports, distributes or otherwise makes or has available, a technical device that has been primarily altered or designed to commit those acts, or 2) manufactures, sells, acquires, imports, distributes or otherwise makes available or has available a computer password, access code or similar information allowing access to an automated work or a part thereof. Lastly, the third paragraph of article 139d DCC states that a person who commits an act as described in the second paragraph of this provision while his intention is aimed at a crime as referred to in Article 138ab, second[61] or third[62] paragraph DCC, is punishable with up to 4 years imprisonment.

Article 139e DCC

1) He who possesses an object he knows, or should know, contains data that is recorded through the unlawful use of eavesdropping, interception or recording of a conversation, telecommunications, data transfer or processing through the use of a computer system,

2) he who gathered data or has become knowledgeable of data that was gathered through the unlawful use of eavesdropping, interception or recording of a conversation, telecom-

---

[60] Criminalizes the use of a DDOS-attack.

[61] The copying, interception or recording of data in a computer system after breaking into that system.

[62] Breaking into a computer system via a public communications network to use the processing capacities of the computer system for one's own benefit or to grant oneself access to a computer system of a third party.

munications, data transfer or processing through the use of a computer system, and subsequently notifies another person of that data, or

3) he who brings the object containing data – as mentioned in paragraph 1 – into the possession of another person, is punishable by up to six months imprisonment.

Article 273a DCC

This provision protects the secrecy of letters by criminalising unlawful opening of letters by persons employed by a postal carrier, which is punishable with up to 18 months imprisonment. The article is a *lex specialis*-provision of article 272 DCC, which criminalises breaching functional and professional secrets.[63]

Article 273b DCC

This provision protects the secrecy of letters by criminalising unlawful discarding of letters by persons employed by a postal carrier, which is punishable with up to 4 years imprisonment, and even 6 years if the content of the letter represents monetary value and said value is appropriated.

Article 273c DCC

Protects the secrecy of telegram messages, by criminalising those who operate a telegraph and intentionally and unlawfully open or share the content of a message, which is punishable with up to 6 months, and criminalising those who intentionally convey the message to a person other than the entitled party or, destroy, discard, appropriate or alter the content of a message, which is punishable with up to 6 years imprisonment.

Article 273d DCC

This provision is meant to protect the secrecy of the telephone, but also encompasses the secrecy of other, new means of communication such as the use of email. It protects data transfer and storage via a public communications network or provider, but in some cases even via non-public networks of providers.[64] The provision is aimed at employees of providers of telecommunications networks and telecommunications providers and breaches of the provision are punishable with up to 18 months imprisonment.

Article 273e DCC

The persons mentioned in the provisions 273a up to 273d DCC, who wilfully allow another person to commit one of the acts mentioned in those provisions or who acts as an accomplice, will be punishable as if he were the one committing those acts.

Article 328quater DCC

If a person (works for a (legal) person who) has a duty to cooperate by providing information concerning telecommunications to the officials of the judiciary or police, or by intercepting or recording these telecommunications, yet accepts a gift or a promise in response to what he has done or neglected or will do or neglect in the execution of said duty, he is punishable with up to 4 years imprisonment, as is the person who provides a gift or a promise to the aforementioned person with such a duty.

---

63 Van der Meij, *T&C Strafvordering*, article 273a Sv, comment 6.

64 Van der Meij, *T&C Strafvordering*, article 273d Sv, comment 9(a).

Article 371 DCC

An official who, while exceeding his authority, is himself presented with or seizes a letter, postcard, document or parcel entrusted to any public body of transport, or a telegraphic message held by a person in charge of the service of a telegraph device that is used for a general purpose, is punishable with up to 2 years imprisonment, as is the official who, by exceeding his authority, is informed by a person working for a provider of a public telecommunications network or service, on any communications traffic that has gone through that network or was transferred by using that service.

2. Telecommunications Act

In addition to the Criminal Code, the TA contains provisions on the protection of personal data and personal privacy. In addition to provisions of the DCCP, Chapter 11 of the TA offers general rules that stipulate that the privacy of personal data, and the 'personal living sphere'[65] in general, has to be guaranteed, especially concerning the processing of data *about* and *of* users and subscribers.[66] To guarantee that these interests are respected, article 11.3 TA orders providers to take technical and organisational measures in light of the safety and security of their networks and services. If – despite these measures – a data leak is determined, article 11.3a TA provides rules on how this should be dealt with, particularly regarding the notification of parties involved. Chapter 11 additionally provides a set of regulations on anonymising specific data, on processing location data and concerning communications that take place on the networks or using the services of public providers, whereas article 11.2a TA specifies that communications of users and subscribers are not to be intercepted, except under certain circumstances such as on court order.

3. Other data protection frameworks

The General Data Protection Regulation[67] that came into force in May 2016 is the primary contemporary legal framework for non-governmental parties on how to deal with and protect personal data. However, this regulation does not regulate personal data collection and protection for police services and judicial authorities as far as this collection takes place in light of maintaining public safety and investigating and prosecuting criminal acts.[68] For police services the Police Data Act[69] is the

---

[65] 'persoonlijke levenssfeer': the national doctrinal principle of the right to respect for private and family life, as given by article 8 ECHR; see also Koops 2016, s. 2.2.2.

[66] Zwenne, *T&C Privacy- en telecommunicatierecht*, chapter 11 Tw, comment 1.

[67] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[68] Further discussion of the Regulation does not fit within the scope of this report.

[69] See Appendix; for further reading on the purpose, possibilities and limitations of this act, see the (English) summary of a study report by the Research and Documentation Centre of the Ministry of Justice and Security (WODC): WODC 2013a, see Appendix.

main legislative act on how to treat data that is gathered in light of their core tasks, whereas the Judicial Data and Criminal Records Act[70] is relevant for the Judiciary, which provides guidelines for the relevant parties on the purpose limitations of personal data.

4. Protection of special contents transmitted by telecommunication

Although no general protection is given to electronic communications concerning business secrets in either the DCCP or any other legal framework, some specific communications are better protected than regular communications. For instance, the communications that are performed by those who have a privilege regarding professional secrecy (the privilege of non-disclosure) – e.g., attorneys-at-law, journalists, notaries and doctors – can only be intercepted by investigation services and used for prosecution under special conditions,[71] which only rarely happens. To try and prevent the interception and recording of communications between a suspect and his lawyer, in 2011 a list was introduced in which phone numbers and other data concerning lawyers can be listed, so that the interception system automatically stops the recording of their communications.[72] In case communications from those with a privilege of non-disclosure are nonetheless recorded, article 126aa paragraph 2 DCCP stipulates that these have to be destroyed. The use of evidence that is extracted from such communications is forbidden and cannot be described in official reports or otherwise end up in the case file, unless special conditions apply.[73] Ignoring this prohibition could lead to the inadmissibility of a case.[74]

C. Powers in the Code of Criminal Procedure

1. The principle of precise parliamentary enactment of public powers in criminal procedure

In the 1990s a crisis erupted in the Dutch investigative landscape because it was revealed that a special police task force, in pursuit of the upper layer of organised crime, used various far-reaching methods that in part were not based on any legal provisions. The upheaval lead to a call for a parliamentary inquiry

---

[70] See Appendix; for further reading on the purpose, possibilities and limitations of this act, see the (English) summary of a study report by the Research and Documentation Centre of the Ministry of Justice and Security (WODC): WODC 2013b, see Appendix.

[71] Article 126aa DCCP.

[72] WODC 2012, s. 3.5.

[73] For further disquisition, see section III.B.3.

[74] Which, for instance, happened in a case concerning 22 suspects linked to the Hells Angels: Rb. Amsterdam 20 December 2007, ECLI:NL:RBAMS:2007:BC0685; for further reading, WODC 2012, s. 3.5 & 6.17.

which, after a thorough investigation, concluded that the legitimacy of Dutch law enforcement was in peril and additional legislation was essential to regain said legitimacy. The legislator responded by introducing a new Act, the Special Investigative Measures Act (hereafter: SIMA),[75] which was inserted into the DCCP and was based on three fundamental principles: (1) the use of special investigative measures must be extensively recorded to allow the judiciary to conduct a proper review of the legality of the employed methods in individual cases, (2) the public prosecutor is responsible for the lawful use of coercive measures, and (3) an infringement of fundamental rights by the government can only be based on codified provisions, whereby the necessity of the infringement must be evident.[76] An elaboration of this last principle results in a limited set of infringing investigative measures that can be used in an investigation, as well as the prohibition of analogous application of said measures; a specific legal provision must be provided that grants the use of a measure for a specific purpose.[77] This principle is in line with article 1 DCCP, which states that criminal procedure only takes place in the manner provided by law.

The regime of special investigative measures that (potentially) infringe human rights is designed as a system of differentiated, precise and specific provisions. An example of a case where this principle was in dispute, was the deployment of an IMSI-catcher[78] ordered by a prosecutor based on article 126nb DCCP[79] to determine the *location* of a suspect. As the provision only allowed the use of an IMSI-catcher to retrieve a user's *communications number*, the Dutch Supreme Court judged[80] that the deployment in this specific case was not based on a specific legal provision in the limited regime of infringing investigative measures; therefore, the prosecutor's order to deploy the measure could not be based on article 126nb DCCP. The legal dispute surrounding the use of the IMSI-catcher does however accurately illustrate the division between minor and serious infringement of Dutch criminal procedure, as the use of the measure in this specific case was eventually not deemed unlawful.[81]

---

[75] See Appendix.

[76] Van Buiten 2016, s. 2.

[77] Explanatory Memorandum to the SIMA, s. 6.1.

[78] An IMSI-catcher ('International mobile subscriber identity') is a device used to intercept traffic data of mobile phone traffic, which can also locate the whereabouts of a mobile device.

[79] In this case, an older version of the still codified provision of article 126nb DCCP was applicable.

[80] HR 1 July 2014, ECLI:NL:HR:2014:1562.

[81] See section below.

2. Differentiation and classification of powers in the Code of Criminal Procedure

In the explanatory memorandum of the SIMA, mention was made of plans to introduce a residual provision specifically designed for the use of coercive measures that are perceived to constitute only minor infringements of fundamental rights when deployed. The idea was cancelled due to major objections and fears that the provision would be too widely used by investigative officers.[82] In the end, it turned out that such a provision was not needed in the SIMA, as other legal provisions already covered the use of less infringing investigative methods; articles 141 and 142 DCCP designate the detection and investigation of criminal offences to the members of the Police Services and the Public Prosecutor, and article 3 Police Act[83] determines that the Police Services are designated to maintain the rule of law. Therein lies the justification of the use of coercive measures that represent only a minor infringement of fundamental rights. Whether or not an infringement is only minor depends on the frequency, duration, intensity, place and way[84] a coercive measure is applied, as well as the intrusiveness of said application, according to the Dutch Supreme Court.[85] An important indicator for testing whether the deployment of a coercive measure is or will be more than a minor infringement, is whether it is *systematic*;[86] if a method will produce a more or less complete image of some aspects of the personal life of a person involved, the use of said method is considered to be systematic. The use of an IMSI-catcher in the previously mentioned Supreme Court case was judged not to be unlawful: under certain conditions the use of such a device during an investigation *can* be more than a minor infringement, but the verdict of the Court of Appeals that – in this specific instance – this was not the case as it was not systematic, was understandable according to the Supreme Court.[87]

As mentioned in previous sections, the Public Prosecutor is the designated authority to lead an investigation and decide on the use of coercive measures to bring the truth to light. The regime of special investigative measures is designed around this principle, divided into three stages. Each specific special investigative measure is described in a separate provision, in which the procedure for acquiring authorisation for the use of the respective measure is described. For the measures that are perceived as only minor infringements, such as a production order regarding user

---

82 Explanatory Memorandum to the SIMA, s. 2.5.

83 Used to be article 2 Police Act during the consideration of the bill.

84 For instance, whether or not technical means are applied, etc.

85 HR 19-12-1995, ECLI:NL:HR:1995:ZD0328, m.nt. T.M. Schalken; also Sackers, *T&C Strafvordering*, article 3 Pw, comment 4(b).

86 Dutch: 'stelselmatig.'

87 HR 1 July 2014, ECLI:NL:HR:2014:1562.

data on a subscriber[88] or CCTV-footage,[89] an investigate officer is independently competent to deploy said measure. Measures that are perceived as more than a minor infringement, such as a production order regarding traffic data of a user of communications services[90] or the use of systematic observation,[91] an investigative officer has to acquire a (production) order from the Public Prosecutor to deploy the measure. Special investigative measures that are perceived to gravely infringe upon fundamental rights, such as the use of infiltration,[92] communications interception[93] or intercepting private (oral) communications using technical means,[94] require an investigative officer to formally ask the Public Prosecutor to obtain an authorization from an investigative judge, only after which the prosecutor can order the use of these measures. The staged distribution of power is therefore not based on a general provision, but specifically attributed to each individual special investigative measure.

III. Powers for Accessing Telecommunications Data in the Law of Criminal Procedure

A. Overview

Within the DCCP, two chapters are of specific importance when it comes to the collection of communications data in investigations; the first being Title IV, dealing with (overt) special coercive measures, the second being Title IVA which deals with (covert) special powers of investigation, the special investigative measures. Within these two chapters several general and specific provisions are provided regarding the acquisition of communications data, of which an overview is given below.

1. Title IV – Special coercive measures

– *Article 125i DCCP*: Allows for (digitally) searching 'data carriers'[95] during the search of 'a place.'

– *Article 125j DCCP*: Is the basis for a network search of a 'computer system'[96] during the search of 'a place.'

---

88 Article 126nc DDCP.
89 Article 126nda DCCP.
90 Article 126n DCCP.
91 Article 126g DCCP.
92 Article 126h DCCP.
93 Article 126m DCCP.
94 Article 126l DCCP.
95 Dutch: 'gegevensdragers.'

– *Article 125k DCCP*: When necessary and if the measures of articles 125i and 125j DCCP are applied, he who is perceived to have knowledge of the mode of security of a computer system, can be ordered to grant access to that computer system or provide information on the mode of security.

– *Article 125l DCCP*: Unless they specifically allow, data *created by* or *for* persons who have a privilege of non-disclosure[97] (e.g., lawyers, journalists) cannot be investigated, and the computer systems on which that data is stored can only be searched in such a way that the professional secrecy is not breached (but, exemptions apply).[98]

– *Article 125la DCCP*: When a search is conducted at a telecommunications network or service provider and data is found that is not meant for or created by the provider, the Public Prosecutor is only allowed to search and store this data if it is evidently from, for or about a suspect, or if the data has led to the crime being committed or has been used to commit the crime.

– *Article 125m DCCP*: If a search leads to the recording or to inaccessibility of data, the persons involved have to be made aware of this recording or inaccessibility as soon as the investigation allows this information to be shared with the persons involved.

– *Article 125n DCCP*: Data that is not relevant for the investigation has to be destroyed, unless exceptions are applicable.[99]

– *Article 125o DCCP*: If, during a search, data is encountered concerning which or with which a crime was committed, the data can be made inaccessible.

2. Title IVA – Special investigative measures

– *Article 126g DCCP*: Forms the basis for systematic observation, which can be used for digitally observing (public) communications (e.g., blogs, forum posts etc).

– *Article 126h DCCP*: Grants the use of infiltration under strict conditions. It can be used to partake in electronic conversations[100] (e.g., infiltrating a criminal organisation and joining and partaking in its Telegram chats).

– *Article 126i DCCP*: Allows the use of pseudo-purchase or -service, which specifically mentions the possibility to acquire, by means of a public telecommunica-

---

[96] Translation by the author of: 'geautomatiseerd werk,' which defines: "a device or a group of interconnected or coherent devices, of which one or more automatically process computer data using a software program."

[97] The groups of persons that have been granted this right are collectively called 'verschoningsgerechtigden' in Dutch.

[98] Section III.B.3.

[99] Which is often the case.

[100] Stein & Rossieau 2003, s. 2.3.

tions network, 'data that is stored, processed or transmitted by a computer system'; this part of the provision is specifically aimed at combatting the internet trade of illegal statements or software.[101]

– *Article 126j DCCP*: Systematic gathering of information finds its legal basis in this provision and entails (actively) approaching individuals to gather information. As is the case with infiltration under article 126h DCCP, it can be used to monitor and partake in electronic communications.[102]

– *Article 126l DCCP*: Stipulates that private communications, that take place without the use of communication service providers (non-mediated), can also be intercepted. Although data has to be *communicated* to be intercepted (which, for instance, means that data that is entered into a computer for personal use cannot be intercepted), the use of a bug on a computer is permitted in order to record data that is *later* communicated via encryption.[103]

– *Article 126la DCCP*: Contains definitions on what constitutes either a provider or a user of a communications service.

– *Article 126m DCCP*: Provides the possibilities for and restrictions on the use of interception of communications via a communications service provider.[104]

– *Article 126ma DCCP*: Deals with jurisdictional issues surrounding the use of communications interception and obliges the notification and approval of another state that is involved.

– *Article 126n DCCP*: Allows the use of a production order for user and traffic data of a person using a communication service.

– *Article 126na DCCP*: Allows an investigative officer to deploy a production order regarding data on a person using a communication service, which includes the name, address, postal code, number and the kind of service the person uses.

– *Article 126nb DC*CP: This provision is the basis for retrieving the number of a user of a communication service by technical means, for instance with an IMSI-catcher.

– *Article 126ng DCCP*: This provision can be used to obtain stored content data from communications providers, such as emails and voicemail-messages.

3. Title V and VB

As mentioned earlier,[105] the DCCP contains three different regimes with the same special investigative measures, each designed for a specific purpose; regular inves-

---

101 Blom, *T&C Strafvordering*, article 126i DCCP, comment 4.

102 Stein & Rossieau 2003, s. 2.3.

103 Blom, *T&C Strafvordering*, article 126l DCCP, comment 3.

104 Will be dealt with extensively infra.

tigations, investigations into criminal enterprises that are committing or planning to commit serious crimes, and the planning or committing of terrorist acts. Titles V and VB cover the use of measures in the last two cases (respectively) and therefore contain the above-mentioned provisions but with different thresholds.

B. Interception of Content Data

1. Statutory provision

The provision on intercepting (tele)communications in Dutch criminal procedure is, as mentioned previously, given in article 126m DCCP, of which the full text is given below:

Article 126m DCCP[106]

1. In the case of suspicion of a serious offence as defined in section 67(1), which serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order, the public prosecutor may, if urgently required by the investigation, order an investigating officer to record by means of a technical device non-public communication that is conducted by use of the services of a provider of a communication service.

2. The warrant shall be in writing and shall state:
   a. the serious offence and if known, the name or otherwise the most precise description possible of the suspect;
   b. the facts or circumstances which show that the conditions, referred to in subsection (1), have been met;
   c. where possible, the number or another indication by means of which the individual user of the communication service is identified as well as, insofar as is known, the name and the address of the user;
   d. the term of validity of the warrant;
   e. a description of the nature of the technical device or the technical devices by means of which the communications are recorded.

3. If the warrant relates to communications which are conducted through a public telecommunication network or by use of a public telecommunication service within the meaning of the Telecommunications Act, the warrant shall – unless such is impossible or is not permitted in the interest of the criminal proceedings – be executed with the assistance of the provider of the public telecommunication network or the public telecommunication service and the warrant shall be accompanied by the request for assistance from the public prosecutor to the provider.

4. If the warrant relates to communications other than the communications referred to in subsection (3), the provider shall – unless such is impossible or is not permitted in the

---

[105] Section 1.A.1.b.bb.

[106] Translation provided by the European Judicial Training Network, http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf; the translation has been edited to match the contemporary provision in the DCCP.

interest of the criminal proceedings – be given the opportunity to assist in the execution of the warrant.

5. The warrant, referred to in subsection (1), may only be issued following written authorization to be granted by the examining magistrate on application of the public prosecutor. At the request of the public prosecutor, the examining magistrate may determine in his authorization that this applies to all numbers or other designations as referred to in the second paragraph, under c, that are in use by the user during the period of validity of the authorization. Section 126l(5) to (8) inclusive shall apply mutatis mutandis.

6. Insofar as is specifically required in the interest of the investigation, the person, who may be reasonably presumed to have knowledge of the manner of encryption of the communications, may be requested, if subsection (1) is applied, to assist in decrypting the data by either providing this knowledge, or undoing the encryption.

7. The request referred to in subsection (6) shall not be directed to the suspect.

8. Section 96a(3) and section 126l(4), (6) and (7) shall apply mutatis mutandis to the request referred to in subsection (6).

9. Rules pertaining to the manner in which the order referred to in subsection (1) and the requests referred to in subsections (3) and (6) may be given and the manner of compliance with such requests shall be set by Governmental Decree.

2. Scope of application

a) Object

As can be seen in the translation given above, the object of interception is *non-public communication that is conducted by use of the services of a provider of a communication service*. The wording of the object of interception allows for a wide interpretation as to what constitutes communication. In addition to fixed communication via landlines and cell phone communications using mobile phones, IP-traffic can be intercepted. The use of an internet tap under Dutch criminal law is performed by intercepting *all* incoming and outgoing internet traffic of an IP-address: Google search terms, streamed movies, chat messages, account names and passwords etc.[107] If only email rather than various types of internet traffic has to be intercepted, it is also possible to request authorization for an email tap, which will only intercept email traffic *to* a certain IP-address.[108] When an interception order for an internet tap has been issued, a provider will pass on all internet traffic data from a specific IP-address (or all traffic from a specific person if a dynamic IP-address is used) to the I&S,[109] which in turn will store it in a secure environment.[110] This data will include person-to-person communication, but also IP-traffic between a person and an automated information system, such as webservers and

---

[107] Oerlemans 2012, s. 'De internettap;' WODC 2012, s. 4.4.

[108] An email tap will only intercept incoming email messages. To intercept outgoing email messages as well, an IP-tap is necessary: WODC 2012, p. 155.

[109] See section I.A.1.c.dd.

[110] WODC 2012, s. 4.

the data transferred to a persons' cloud storage.[111] Even if the person behind an IP-address is not actively involved in the transfer of data to an automated information system, for instance when two automated machines communicate in light of the 'Internet of Things,' the communications will be caught when passing the internet service provider. An important technical restriction to the use of an internet tap is the fact that only electronic communications will be intercepted that go through the network of the Internet Service Provider, or *access provider* (which is also increasingly encrypted). This means that peer-to-peer communication, which does not always (fully) flow through a central server, might not (always) be interceptable through the use of article 126m DCCP.[112]

An important criterion for the interception of communications is whether the data is in transit. Only streaming data can be intercepted; as soon as communications data is stored, investigative measures other than those of article 126m DCCP have to be used to gather the data. For instance, stored (draft) e-mails or stored private messages sent via social-network services (Facebook, Twitter),[113] services which *can* fall into the category of providers of a (public) communications service, have to be demanded with a production order based on article 126ng paragraph 2 DCCP.[114] If a provider is considered not to be a communication service provider as defined in provision 126ng DCCP, which is in debate for providers like Skype and Gmail because it is contested whether they are electronic communications providers as defined in the Dutch Telecommunications Act,[115] or if the holder of sent mail is not a provider at all (i.e., the recipient), the general measure on 'demanding content data'[116] provided in article 126nd DCCP has to be used.[117] Whether or not data is *in transit* or *stored*, and whether the definition of a (public) provider of a communication service is too narrow in light of recent developments in the field of communications technology,[118] are questions that have resulted in quite some doctrinal debate.

b) Current matters of dispute

Within the framework of special investigative measures and other relevant provisions, a clear distinction is made regarding data considered to be in transit and data

---

111 Koops 2012a, s. 5.1.3.

112 Oerlemans 2012, s. 'De taplast.'

113 Oerlemans 2012, s. 'Verkeersgegevens en gegevens bij communicatieaanbieders.'

114 Blom, *T&C Strafvordering*, article 126ng DCCP, comment 1.

115 Oerlemans 2012, s. 'De taplast.'

116 Article 126nc DCCP provides the measure of requesting identifying data via a production order, whereas article 126nf DCCP deals with a production order on sensitive data and article 126nd DCCP deals with (regular) content data.

117 Koops 2012a, s. 5.1.2.

118 The latter question will be discussed in the next section, but also further discussed in section III.B.4.a. and b.

that is stored. As was seen in the previous section, not all communications providers are considered to be communications providers as meant in various legal frameworks concerning communications, which causes inconsistencies in the application of the special investigative measures; if, for instance, email messages are stored by a communications provider as meant by the official definition, these messages have to retrieved by using article 126ng DCCP, which stipulates that an authorization by an investigative judge is compulsory, whereas retrieving similar emails from a provider that is not considered to be such a communications provider (e.g., certain cloud services[119]), these messages can be retrieved using the production order of article 126nd DCCP, which does not require judicial authorization. Furthermore, the crimes for which the respective measures can be deployed differ substantially. Koops *et al*. argue that this discrepancy requires clarification and rectification.[120] The legislator has already recognised the fading of the clear distinction between stored data and data in transit,[121] but so far has been unable to provide a definitive solution. A committee tasked with advising the legislator on modernising the DCCP in light of investigations in a rapidly digitizing society, emphasised that this differentiation no longer fits the contemporary communications landscape and provides suggestions on how the constitutional safeguards regarding communications can be applied in this respect.[122] The Koops Committee also signalled another, related issue; incoming messages on a seized device. Particularly in the case of seizure of smartphones, data such as text messages (can) still pour in on a device if the network connection of the device is not terminated, or is turned on again. Whether it is permissible to take cognizance of new substantive data that arrives on or via an automated work or digital data carrier after confiscation or during a network search, is a matter that has not been dealt with appropriately by the legislator, the Koops Committee has concluded.[123] According to the committee, the problem that should be addressed is the fact that this data can be viewed as *data in transit* while this data is retrieved by the authorities by seizure (not interception) *and* without involvement of an investigative judge. The Committee believes that the data coming in during the short, natural period between seizure and disconnection is pure 'bycatch,' for which no additional authority or standardization is required, but – depending on the extent to which the investigative officers actively contribute to the collection of such new data – it is possible that the constitutional protection of data in transit will be infringed, which should require the authorization of an investigative judge. In general, the Committee believes that the legislator must pro-

---

119 See section III.B.5.a.

120 Koops 2012a, s. 5.2.2.

121 Explanatory Memorandum to the Computer Crimes Act III, s. 2.2.

122 Koops Committee Report 2018, s. 6.3.3. An English summary of the Koops Committee Report will become available in the course of 2019: Koops Committee Report 2018.

123 Koops Committee Report 2018, p. 197.

vide means to take note of later incoming messages, provided that this is adequately standardized.[124]

Whether these suggestions – given above in light of the different matters in dispute – will be processed into the revision of the DCCP, which is planned to be implemented sometime in the next decade, or whether these suggestions will lead to earlier adaptations to the current framework, is yet unclear.

3. Privileged information

a) Overview

Dutch legislation surrounding the interceptability of communications offers relatively few restrictions on which types of information can be obtained by the investigative authorities. Any kind of information a suspect, or any person involved, shares through the means of communication can be used in the investigation and prosecution of suspects; no specific prohibitions regulate the use of data that stem from the *core area of private life* such as data regarding prayers, sexual activities or from diaries. However, the DCCP and other relevant bodies of legislation do protect communications with certain professionals; therefore, some specific types of communications are better protected than regular communications. Examples of these communications are those in which a person partakes who has a privilege of non-disclosure. The provision on those who are subject to professional secrecy is that of **article 218 DCCP**:

> Those persons who have a duty of secrecy by reason of their position, profession or office may also assert privilege when called to testify or answer certain questions, but only in regard of information entrusted to them in their aforementioned capacity.

Among the limited list of persons who can be viewed as covered by this provision are the doctor, the clergyman, the notary and the attorney-at-law. Other medical practitioners than doctors may also be entitled to privilege, such as the pharmacist, the midwife and the nurse.[125] Their communications can only be intercepted by investigation services under special conditions,[126] and such interception only rarely happens. To try and prevent the interception and recording of communications between a suspect and his lawyer, in 2011 a list was introduced in which phone numbers and other data can be listed concerning those with an attorney-client privilege, so that the interception system automatically stops recording their communications.[127] In case such communications are nonetheless recorded, article 126aa paragraph 2 DCCP stipulates that these have to be destroyed. The use of evidence that is extracted from such communications is forbidden and cannot be

---

[124] Koops Committee Report 2018, s. 5.3.4.

[125] Van der Meij, *T&C Strafvordering*, article 218 DCCP, comment 2.a.

[126] Article 126aa DCCP.

[127] WODC 2012, s. 3.5.

described in official reports or otherwise end up in the case file.[128] The public prosecutor is responsible for the correct destruction of the evidence gathered and the official reports based thereon. Ignoring the prohibition on the use of this evidence can, in serious cases, lead to the inadmissibility of the case.[129]

The fact that persons have a right to professional secrecy does not, however, automatically mean that communications involving them are *not* interceptable *in any situation*, as can be seen in the next subsections concerning interception of communications surrounding lawyers and journalists.

b) Journalists

Although the question whether journalists are covered by the privilege has been the subject of debate for several years, the ECtHR decisions in *Goodwin*[130] might represent a turning point in the sense that there is now a Designation on the use of coercive and investigative measures against journalists.[131] It states that it is generally unlawful to use coercive measures against a journalist to discover the identity of a source. However, a breach of this right to source protection is possible under special circumstances: when disclosure of the source is necessary in a democratic society, in view of one or more of the interests mentioned in article 10 paragraph 2 ECHR.'[132] With the introduction of the Source Protection Act[133] in October 2018, the right of journalists to protect their sources was solidified in article 218a DCCP, which states that witnesses who, as journalists or publicists in the context of news gathering, have access to data from persons who have provided this information for disclosure, may be exempted from answering questions about the origin of such data.[134] The investigative judge may reject the invocation of this right if he considers that disproportionate damage would be caused if questions of a weightier public interest were left unanswered.[135] Article 126aa DCCP has been adapted and now also states that official reports and other items in which information is provided concerning those persons mentioned in article 218a DCCP (journalists and publicists), have to be destroyed. This also concerns the content gathered by the use of interception measures.

---

128 Unless special circumstances apply, see further subsections.

129 Which, for instance, happened in a case concerning 22 suspects linked to the Hells Angels: Rb. Amsterdam, 20 December 2007, ECLI:NL:RBAMS:2007:BC0685; for further reading, WODC 2012, s. 3.5 & 6.17.

130 ECtHR, *Goodwin v United Kingdom*, 11 July 2002, no. 28957/95.

131 See Appendix.

132 Which is stipulated in article 218a DCCP, see Designation on the use of coercive and investigative measures against journalists, s. 1.3 (see Appendix). Also Van der Meij, *T&C Strafvordering*, article 218 DCCP, comment 2.c.

133 See Appendix.

134 Article 218a para. 1 DCCP.

135 Article 218a para. 2 DCCP.

c) Attorneys-at-law

Before the Special Investigative Measures Act (SIMA)[136] codified the wide range of investigative measures into the DCCP, there was already a provision that dealt with the use of an interception measure. This provision, article 125g DCCP (old), used to stipulate that only communications in which a suspect took part, could be intercepted. The Supreme Court, given a case in which the communications of a lawyer were intercepted, judged that those who are entitled to professional secrecy could only be intercepted if they themselves were suspects.[137] The framework of this judgment in combination with a Designation concerning the use of investigative and coercive measures against lawyers,[138] which was introduced in relation to the SIMA, must lead to the conclusion that these restrictions still apply, according to Lintz and Verloop.[139] A later version of the Designation confirms that only in special circumstances is the interception of communications between an attorney and his client lawful, which is the case if the attorney is a suspect himself.[140] If such circumstances are not present but such communications are intercepted nonetheless, they will have to be destroyed.[141] The information that has become known through the unlawful interception cannot be used in any way within the investigation.[142]

4. Execution of communications interception

Within the DCCP two main provisions deal with the interception of communications, which are provisions 126m and 126l. The first is designed for intercepting communications that are taking place through the use of the services of providers, whereas the latter is meant for private communications *not* via service providers.

a) Execution by the authorities with the help of third parties

When communications are taking place via the use of networks or services of access providers, article 126m DCCP is the main provision based on which the com-

---

136 See also section II.C.1.

137 HR 12 September 2006, ECLI:NL:HR:2006:AV6188, *LJN* AV6188; Lintz & Verloop, Het professioneel verschoningsrecht: soms zijn er grotere belangen dan de waarheidsvinding in strafzaken, 4.2.

138 Designation concerning the use of investigative and coercive measures against lawyers (see Appendix).

139 Lintz & Verloop 2009, s. 3.3.

140 Designation concerning the use of investigative and coercive measures against lawyers; also HR 10 December 2013, ECLI:NL:HR:2013:1740, *NJ* 2014/93, m.nt. F. Vellinga-Schoostra; Kroon-Van Zweeden 2015, s. 2.1 and 5.1.

141 Article 126aa para. 2 DCCP.

142 Designation concerning the use of investigative and coercive measures against lawyers.

munications can be intercepted, provided that the formal and substantive requirements are fulfilled. In general, electronic communications are intercepted by ordering the network and service providers to extract and surrender the requested electronic communications that run through either telephone or IP-lines. The definition of which (legal) persons qualify as a provider of a communications service, which includes providers of communications networks,[143] can be found in definition provision **article 126la DCCP**:

> The natural person or legal person who/which, in the practice of a profession or conduct of a business, provides the users of his/its service with the possibility of communicating by means of a computerised device or system, or processes or stores data for such a service or for the users of that service;[144]

The Regulation for the interception of public telecommunications networks and services[145] provides an overview of which communications means are to be seen as public telecommunications networks and services, which include fixed public telephone networks and services, lease lines, GSM, DCS 1800, GPRS, ERMES, TFTS, internet and IMT-2000.[146] The Regulation further offers specific design requirements for the respective means of communications with regard to interceptability.[147]

b) Execution by the authorities without the help of third parties

It is not necessarily preferable in all circumstances to make use of cooperation duties that apply to telecommunications providers. The mere sending of a production order to a provider could potentially endanger the investigation. The legislator has anticipated this problem and provided the possibility to intercept electronic communications via a provider without its cooperation (or knowledge of the interception).[148] Paragraph 3 of article 126m DCCP states that the interception of such communications should be executed in cooperation with providers, except in cases where this is not possible or if the interests of criminal procedure oppose it. This general rule, which stipulates that interception measures should be deployed in cooperation with providers except under special circumstances, does not apply to providers of private networks as the risk of damaging the investigation is far great-

---

[143] Blom, *T&C Strafvordering*, article 126la DCCP, comment 1.

[144] Translation provided by the European Judicial Training Network, http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf

[145] See Appendix.

[146] Article 2 Regulation for the interception of public telecommunications networks and services.

[147] Article 3 Regulation for the interception of public telecommunications networks and services.

[148] *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 42; Borgers & Kooijmans, Het Nederlands strafprocesrecht, XII.13 Onderzoek van communicatie via een aanbieder van een communicatiedienst.

er.[149] Furthermore, these types of providers will often have less technical capacity to intercept communications (and are not required to be interceptable). When no cooperation is sought in the execution of an interception order, the technical means that are used to intercept communications are subject to strict(er) conditions.[150] Although specific information is very limited on what such interception would constitute, no specific provision prohibits the interception of cables, WLAN, satellite communications or the use of remote forensic software. Examples of techniques that are used to intercept communications in this context, are Wifi- and IMSI-catchers.[151]

Stricter conditions will be applicable to this type of interception, as the use of special investigative measures are bound by the general principles of precise parliamentary enactment of public powers in criminal procedure and the principles of due process. Also, when targeting specific means of communication, the division between the provisions of article 126m and 126l DCCP will have to be kept in mind, as the former is meant for mediated communications (therefore, via electronic communications networks) and the latter for private communications.[152] Furthermore, the provision on *remote* hacking (and therefore, the use of remote forensic software) as a special investigative measure is yet to enter into force, potentially limiting the possibilities regarding this topic.[153]

c) Specific jurisdictional issues relating to intercepting communications via a provider

Article 126ma DCCP, which was implemented in 2006 in light of article 20 paragraph 2 of the EU MLA Convention, stipulates specific conditions for the use of the interception measure of article 126m DCCP with regard to communications that partly take place outside Dutch jurisdiction:

Article 126ma DCCP

1. If on issuance of a warrant as referred to in section 126m(3), the user of the number, referred to section 126m(2)(c), is known to be located in the territory of another state, that other state shall be informed of the intention to record telecommunications and the permission of that state shall be obtained before the warrant is executed, insofar as is prescribed under a treaty and in application of that treaty.

2. If after the start of the recording of telecommunications on the basis of the warrant it becomes known that the user is located in the territory of another state, that other state

---

149 Corstens/Borgers & Kooijmans 2018, chapter XII.13.

150 Designation on investigative powers 2014, referring to Decree on telecommunications provision 2006.

151 Designation on technical means in criminal procedure 2006, section 2.d.

152 For instance, non-public radio traffic should be intercepted using 126l DCCP: Ter Haar & Van den Brink 2018, s. 3.10.

153 For further discussion on the topic of hacking, see section III.D.1.

shall be informed of the intention to record telecommunications and the permission of that state shall be obtained, insofar as is prescribed under a treaty and in application of that treaty.

3. The public prosecutor may also issue a warrant as referred to in section 126m(3), if the existence of the warrant is necessary in order to be able to request another state to record telecommunications by means of a technical device or to intercept telecommunications and directly transmit them to the Netherlands for the purpose of recording by means of a technical device in the Netherlands.[154]

d) Interception of confidential (oral) communications

The use of the 'regular' interception measure, which deals with intercepting communications that are performed via the networks and services of communication providers, is bound by the interception of those *networks*. No accompanying powers permit entrance into confined spaces, e.g., houses or offices, to intercept these mediated communications. In addition to a general provision on covertly entering a confined space (excluding homes) that is given in article 126k DCCP,[155] the provision on intercepting confidential communications of article 126l DCCP (on intercepting direct/oral communications in contrast to mediated communications via article 126m DCCP) offers the possibility to enter confined spaces specifically meant for intercepting communication using technical means:

Article 126l DCCP

1. In the case of suspicion of a serious offence as defined in section 67(1), which serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order, the public prosecutor may, if urgently required in the interest of the investigation, order an investigating officer as referred to in section 141(b) (c) and (d) to record confidential communications by means of a technical device.

2. The public prosecutor may, in the interest of the investigation, determine that an enclosed place, not being a dwelling, will be entered without the consent of the person entitled to use the premises for the purpose of executing the warrant, if urgently required in the interest of the investigation and in the case of a serious offence which carries a statutory term of imprisonment of at least eight years, he may determine that a dwelling will be entered without the consent of the person entitled to use the premises for the purpose of executing the warrant. Section 2(1, last sentence) of the General Act on Entry into Dwellings shall not apply.

---

[154] Translation provided by the European Judicial Training Network, http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf. The translation has been edited to match the contemporary provision in the DCCP.

[155] Although it is permitted to record sound and images during the execution of this measure, it is not permitted to record confidential communications during the execution of this measure: Blom, *T&C Strafvordering*, article 126l DCCP, s. 7.c. The measure has a limited set of purposes, which are the recording of a place, the securing of traces and the placing of a technical aid in order to be able to determine the presence or movement of a good: Blom, *T&C Strafvordering,* article 126l DCCP, comment 9.

3. The warrant to record confidential communications shall be in writing and shall state: a. the serious offence and if known, the name or otherwise the most precise description possible of the suspect; b. the facts or circumstances which show that the conditions, referred to in subsection (1) and, if subsection (2, second sentence) applies, the conditions referred to in subsection (2), have been met; c. at least one of the persons who participate in the communications, or, if the warrant relates to communications in an enclosed place or in a means of transport, one of the persons who participate in the communications or the most precise description possible of that place or that means of transport; d. in the application of subsection (2), the place to be entered; e. the manner in which the warrant will be executed, and f. the term of validity of the warrant.

4. The warrant may only be issued following authorisation to be granted by the examining magistrate on application of the public prosecutor. The authorisation shall relate to all elements of the warrant. If a dwelling may be entered for the purpose of executing the warrant, that power shall be explicitly 54 stated in the warrant.

5. The warrant shall be issued for a period of maximum four weeks. The term of validity may be extended for a period of maximum four weeks each time.

6. Section 126g(6) to (8) inclusive shall apply mutatis mutandis, on the understanding that the public prosecutor shall require authorisation from the examining magistrate for amendment, supplementation or extension. If the public prosecutor determines that a dwelling will be entered for the purpose of executing the warrant, the warrant may not be issued verbally. As soon as the conditions, referred to in subsection (2, second sentence), are no longer met, the public prosecutor shall determine that the execution of the warrant is terminated.

7. In the case of urgent necessity, authorisation from the examining magistrate, referred to in subsections (4) and (6), may be granted verbally, unless subsection (2, second sentence) is applied. In that case the examining magistrate shall put the authorisation in writing within three days.

8. An official report on the recording shall be prepared within three days.[156]

In the execution of an interception order based on this provision, houses can be entered to facilitate the interception of confidential communications; for example to install microphones or to place bugs in computers that record keystrokes and mouse clicks.[157] For further elaborations on the possibilities and limitations that concern the deployment of the measure provided in article 126l DCCP, see section III.D.1.

5. Duties of telecommunication service providers to cooperate

a) Overview

In the previous section it was briefly mentioned that the execution of interception orders based on judicial warrants is generally performed in (mandatory) coopera-

---

[156] Translation provided by the European Judicial Training Network, http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf. The translation has been edited to match the contemporary provision in the DCCP. Underlining provided by author.

[157] Blom, *T&C Strafvordering*, article 126l DCCP, comment 1.

tion with service providers. Telecommunications *network* and *service* providers are both obliged to cooperate in the interception of communications that respectively go through their networks or are based on their services, which is based on article 13.2 TA. As was already stipulated in the previous section, the definition of which (legal) persons qualify as a provider of a communications service – which includes providers of communications networks[158] – can be found in definition provision **article 126la DCCP**:[159]

> The natural person or legal person who/which, in the practice of a profession or conduct of a business, provides the users of his/its service with the possibility of communicating by means of a computerised device or system, or processes or stores data for such a service or for the users of that service.[160]

The result of the given definition, which is derived from the considerations in the Cybercrime Convention,[161] is fairly broad and encompasses a wide range of providers,[162] although for some categories it is in debate whether they fall under the given definition. For example, a person, who uses his computer at home to create a webserver on which family members can host a website, is not covered by the definition of 'a provider of a communications service.'[163] Another problem, which is extensively described by Oerlemans, is the fact that the Telecommunications Act[164] only requires *public* telecommunications to be made interceptable by their providers, which could lead to problems regarding intranet-connections within closed groups, such as companies or a network of institutions.[165] A side note here is that article 126m DCCP mentions that communications that take place other than via *public* providers, can still be intercepted.[166] In that case, the provider should be offered the chance to cooperate in the interception unless this is impossible or when it might pose a risk to the investigation.

---

158 Blom, *T&C Strafvordering*, article 126la DCCP, comment 1.

159 When the Computer Crimes Act III enters into force – which has momentarily (January 2019) been postponed – this provision will be replaced by article 138g DCCP.

160 Translation provided by the European Judicial Training Network, http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf.

161 Convention on Cybercrime, see Appendix.

162 Research in 2005 and 2009 suggests that, in general, telecommunications are fairly interceptable: Koops 2005; Stratix 2009.

163 Blom, *T&C Strafvordering*, article 126la DCCP.

164 See section II.B.2.

165 For example, a network of scientific and educational institutions, which was using an intranet service, Surfnet. The lower court in Rotterdam judged (in summary proceedings) that its communications services was not covered by the definition of *public* telecommunications, as it was not offered to the general public but to a select group of people: Rb. Rotterdam 27 March 2009, ECLI:NL:RBROT:2009:BH9324; Oerlemans 2012, s. 'De taplast.'

166 Article 126m para. 4 DCCP.

Oerlemans also signals a problem surrounding the definition of a *provider*: the Telecommunications Act[167] defines a telecommunications *service* as 'a service that consists wholly or partly in the transmission or routing of signals via an electronic communication network, in so far as this does not consist of distributing programs'.[168] The basic services of providers like Skype, which use an existing telecommunications infrastructure to offer its users encrypted communication services but which are not chiefly offering the actual transfer or routing of signals, are not covered by the Telecommunications Act, according to Oerlemans.[169] This also applies to hosting-, proxy service-, VPN- and storage providers.[170] Gmail and Hotmail are also not considered to be providers of electronic communications services, as they usually are not the ones who transmit the signals from which these email services exist via electronic communication networks.[171]

In light of the above-mentioned bottlenecks, the Koops Committee formulated a number of recommendations for the legislator to keep in mind during the modernization process of the DCCP: the legislator should as a minimum change the definition of 'provider of a communications service' in such a way that hosting providers, for whom providing communications is merely an additional service to offer its clients, are also encompassed.[172] The discussion on data that is either stored or in transit, as mentioned in section III.B.2.b., also constitutes an array of problems with respect to cooperation duties, as it is often unclear whether data from a subject is either in transit or stored at, say, a cloud-provider. Which measures to use in such cases and which measures the providers are mandated to cooperate with, can be subject to debate. As the use of these new semi-communications services will most likely rise exponentially in the near future, this is a somewhat urgent problem that needs to be addressed by the legislator.

b) Description and regulation of cooperation duties for providers

The DCCP requires in several, specific provisions that providers have to cooperate with authorities. Furthermore, the Telecommunications Act states that provid-

---

167 Article 1.1, under ff, Telecommunications Act.

168 Translation by the author.

169 Apart from the problems surrounding jurisdiction.

170 Knol en Zwenne, *T&C Privacy- & telecommunicatierecht*, p. 371; Amendment to the Telecommunications Act due to Directive 2002/58/EG, p. 6; Detailed Statement of Response concerning the Amendment to the Telecommunications Act due to Directive 2002/58/EG, p. 4; Oerlemans 2012, s. 'De taplast;' Koops & Oerlemans 2019, s. 3.4.7.

171 CBb 3 December 2014, ECLI:NL:CBB:2014:438, s. 4.1.8; Knol, *T&C Privacy- en telecommunicatierecht*, article 1.1 TA, comment 17.

172 As the initial draft proposal for the modernization of the DCCP only covered providers for whom a communications service was the main business activity; Koops Committee Report 2018, s. 5.6.

ers[173] have to cooperate *and* provide networks and services that are interceptable. These duties to which providers have to adhere are fairly broad and unspecified; specifications of what the duties entail can be found in lower legislation, such as the Decree on interception of public telecommunications networks and services[174] and the Regulation for the interception of public telecommunications networks and services.[175] Provision 2 of the Decree offers an overview of the requirements that have to be fulfilled by the providers of communications networks and services with regard to interceptability. It stipulates, among other things, that 1) a production order concerning interception must be carried out as indicated in the documents, 2) the interception should not be noticeable by the user or others involved, 3) the acquired information must be transferred to the authorities immediately and 4) without encryption or other restrictions that were put in place by that provider. Provisions 3 and 4 of the Decree determine that further requisites will be provided in ministerial regulations, of which the aforementioned Regulation is an example. The Regulation offers specific design requirements for the respective means of communications with regard to interceptability,[176] as well as technical requirements.[177] Regarding design requirements, providers are required to arrange their network or services in such a way, that an interception order can be executed immediately if the order contains data on the user's account name, his identifying number or his electronic mail address, as provided to that user by the provider concerned.[178] The information that is passed down by the provider to the authorities must meet several technical requirements, protocols and formats: 1) it must encompass all signals that are sent to and received from the network connection point or by the user, 2) it must be provided with identifying data on the network connection points or of the user, and 3) the data must be handed down via secure networks/connections or be encrypted (where the means of transit are subject to official consent by authorities, in order to protect the security and reliability of the connections and the protection of personal data).[179, 180] Technically, the transfer of intercepted communications from providers to the authorities (I&S) within Dutch criminal procedure is subject to protocol duties provided in the Transport of Intercepted IP Traffic (TTIP) protocol and the ETSI-IP handover interface of the European Telecommunications Standards Institute (ETSI).[181, 182]

---

173 That fall within the definition of 'public providers'.

174 See Appendix.

175 See Appendix.

176 Regulation for the interception of public telecommunications networks and services, para. 2.

177 *Ibid.*, para. 3.

178 *Ibid.*, article 8.

179 *Ibid.*, article 12.

180 *Ibid.*, articles 10 and 11.

181 https://www.etsi.org/

c) Requirements for providers on securing gathered data

While the previously discussed Decree specifies what the cooperation duty entails for providers, the Decree on securing data on telecommunications[183] specifies the requirements the providers should adhere to regarding the security of gathered data. Providers have to take the necessary security measures to prevent unauthorized inspection of information and data gathered in cooperation with intelligence services or in light of criminal investigations, which entail measures regarding: their personnel, data storage buildings and spaces, their information systems, possible calamities and the breach of confidentiality of the gathered data and information.[184] These requirements are further specified in an Appendix to the Decree[185] and will also be discussed in section III.B.11.

d) Requirements for providing (other) data to authorities by providers

As will be discussed further in section III.C.1.d., user data concerning a user (or subscriber) of a communication service is to be accessible for investigative officers via the Central Information Desk for Research on Telecommunications (CIOT).[186] Each police unit has a special computer which only authorized investigators can use to gain access to the CIOT-system. With this system, the data – which is mandatorily updated every 24 hours by the communications services[187] – can be consulted fully automatically.[188] The providers of internet services are to know who the user is behind a dynamic IP address and will have to be able to provide data that is demanded by investigative officers through the use of a production order.[189] The data has to be provided to the CIOT in specific formats concerning personal data[190] and addresses.[191, 192] Another requirement providers have to adhere to, is

---

182 As stipulated by the Agency Telecom (Agentschap Telecom) of the Ministry of Economic Affairs and Climate, see https://www.agentschaptelecom.nl/onderwerpen/telecom aanbieders/aftappen-van-gegevens.

183 See Appendix (first version entered into force on 1 June 2005).

184 Article 2 Decree on securing data on telecommunications 2018.

185 Appendix to article 2 para. 3 Decree on securing data on telecommunications 2018.

186 CIOT is part of the Ministry of Justice and Security and is the link between investigation services and telecom companies and is responsible for the storage and use of identifying data: WODC 2012, p. 12.

187 Every 24 hours, a provider has to provide a digital file containing the up-to-date data on its subscribers: article 4 para. 2 Decree on telecommunications provision 2000.

188 Blom, *T&C Strafvordering*, article 126n DCCP, comment 7.

189 Some providers can connect an internet tap on the basis of a name, address, and place of residence: WODC 2012, s. 4.4.

190 NEN 1888.

191 NEN 5825.

192 Appendix Decree on telecommunications provision, para. 2.

that they should be able to perform a data analysis[193] based on which the number of a specific person can be retrieved: instead of using an IMSI-catcher,[194] investigative officers can also request (after authorization from the public prosecutor)[195] a provider to determine which phone number was used on two (or more) separate occasions. When the officers have observed that a person of interest (whose number has yet to be retrieved) has used his communications device on separate occasions in specific locations, an analysis of all communications traffic on those occasions in the respective locations will likely produce only one specific communications number which has been used on all occasions; it must therefore be the number of the person of interest. If the person of interest has used his device in a remote area, even an analysis of the communications traffic of that specific moment and location might suffice.[196]

6. Formal prerequisites of interception orders

a) Competent authorities

As mentioned in previous paragraphs, the division of powers in the system of the DCCP is such, that special investigative measures only capable of minor infringements can be deployed by investigative officers. Measures capable of great infringement require prior authorization by the Public Prosecutor and the measures capable of the most grave infringements require authorization by an investigative judge. The application for a communications interception order belongs in the last category, as intercepting communications is perceived as a grave infringement of the privacy of subjects. Whether or not one of the parties involved in the communications has consented to the interception of said communications, does not play a role in whether an order has to be obtained: an order must always be applied for. The prescribed procedure cannot be circumvented by enticing one of the conversation participants to record the conversations himself, as this would conflict with rulings of the ECHR.[197]

---

193 'Bestandsanalyse.' The requirement is given in article 13.4 para. 3 TA.

194 See section III.C.2.

195 Based on article 126na para. 2 DCCP.

196 See Koops & Oerlemans 2019, s. 3.3.2.

197 In any case, the ECtHR judges this unlawful when it is done at the direction of the police: ECtHR, *M.M. v. The Netherlands*, 8 April 2003, no. 39339/98, *NbSr* 2003/185; ECtHR, *Van Vondel v. The Netherlands*, 25 October 2007, no. 38258/03, *NJ* 2008/584, m.nt. Dommering. In Dutch case law, a similar reasoning can be found: HR 26 May 2009, ECLI:NL:PHR:2009:BH8800, *NJ* 2009/261. See also Reijntjes 2017, s. 4.11.3.2.

b) Formal requirements for applications

The procedure regarding applying for an interception order is explained in paragraph 1 of article 126m DCCP, which states that a Public Prosecutor can order an investigative officer to intercept non-public communications via a provider of communications services. To be able to order the interception, a public prosecutor does however require prior authorization of an investigative judge, according to paragraph 5 of article 126m DCCP. Paragraph 2 describes the formal requirements that should be encompassed in the text of an order to meet the legal standards. It should mention:

a) the suspected crime that is investigated and the name or a description of the suspect that is as accurate as possible,
b) the facts or circumstances from which it appears that the requirements referred to in the first paragraph have been fulfilled (these requirements are the substantive prerequisites that will be dealt with in the next paragraph),
c) if possible, the number or other indication identifying the individual user of the communication service and, as far as is known, the name and address of that user,
d) the period of validity of the order, and
e) an indication of the nature of the technical aid or the technical aids with which the communication is recorded.

In practice, an investigative officer writes an application – as is done for the use of any special investigative measure – in which an overview is given of the criminal acts a person is suspected of, all previously performed (relevant) investigative actions and their results, as well as relevant data on the communication that is to be intercepted. The application will subsequently be sent to the public prosecutor, at times accompanied by other relevant and related official reports. The prosecutor will check whether the formal and substantive prerequisites have been met. As the officer is subject to a professional oath, which entails (among others) that his statements are to always be completely accurate and reliable, there is generally no doubt about the sincerity of the application text. However, sometimes a prosecutor will ask for related reports or documents, to check whether everything is accurately portrayed. As soon as the prosecutor is satisfied that all requirements are met, he can decide to request an authorization from the investigative judge, which is also done in writing. The written request and the application are then sent to an investigative judge, who will perform his or her own check regarding the substantial and formal prerequisites and will subsequently decide whether or not the use of the interception measure is authorized. If it is, a written authorization is sent back to the public prosecutor, who in turn will register the authorization and produce a written order and a written production order. The order is directed towards the investigative officers, which orders them to deploy an interception measure as requested, and the production order is directed towards the communications service provider (of which the person to be intercepted is a subscriber), and demands its

cooperation in the interception of a subscriber's communications. All documents produced by the public prosecutor and the investigative judge are sent to the investigating officers, who will then be able to start intercepting. This is done by directing all the paperwork to the I&S.[198] The I&S will check whether the formal requirements have been met, after which it will start the recording of the communications.

c) Cases of emergency

In cases of emergency the process described above can be done orally:[199] The investigating officer will call the prosecutor and explain what has happened and why it is necessary to immediately receive an interception order. If the prosecutor is satisfied that all the formal and substantive prerequisites have been met, he will call the investigative judge. The judge will then give an oral authorization for the interception if he is also satisfied that the prerequisites have been met. The prosecutor can then call the I&S to order them to start intercepting. Within three days the application, production orders, the authorization and the order that have been given, will have to be put in writing.[200] If this requirement has not been met within that time, the I&S will stop the interception immediately.

7. Substantive prerequisites of interception orders

a) Overview

The prerequisites that have to be fulfilled before an interception authorization can be granted, are twofold; in addition to the formal prerequisites dealt with in the previous section, substantive prerequisites are in play as can be seen in the text of the provision. An important test for granting an interception authorization is whether the intrusiveness of the measure on those subjected to interception is outweighed by the seriousness of the criminal suspicion. The degree of suspicion, the person against whom an investigative power can be deployed, the duration of deployment, the procedure of authorization and the grounds on which a special investigative power can be used, can say something about the extent to which the measure is perceived as intrusive.[201]

---

198 See section I.A.1.c.dd.

199 Article 126m para. 8 DCCP says that article 126l para. 7 DCCP applies accordingly, which states that in urgent cases the investigative judge can give an oral authorization, provided that the order will be put in writing within 3 days.

200 See para. 8 of article 126m DCCP in combination with para. 7 of article 126l DCCP.

201 WODC 2012, p. 19.

b) Degree of suspicion

The first substantive prerequisite represents both the degree of suspicion needed and the type of crimes that can warrant the use of an interception measure. The degrees of suspicion are threefold in Dutch criminal proceedings: sometimes it suffices that there is an *indication* that a crime has been or is being committed,[202] but normally there has to be a reasonable presumption or *suspicion*[203] towards a person – the person in whose respect facts or circumstances give rise to a reasonable suspicion of guilt of a criminal offence.[204] Some measures capable of a grave infringement of rights, like placing a person in pretrial detention, require an even higher degree of suspicion as there have to be grave presumptions towards a suspect: there has to be a high degree of probability that the suspect has committed a criminal offence.[205] For a successful application of an interception warrant, there must be a *suspicion* of a criminal act for which pre-trial detention is permitted. As is already mentioned section I.A.1.b.cc., a reference is made in the provision on communication interception to criminal acts described in paragraph 1 of article 67 DCCP. This provision mentions all the criminal acts for which suspects can be placed in pre-trial detention. Generally, this is for all criminal acts that are punishable with at least four years imprisonment, but over the years several other crimes with lower maximum sentences, like embezzlement,[206] scamming,[207] and threatening with any crime against life,[208] have been added to the list.[209]

c) Principle of proportionality

When the first criterion, the suspicion of a serious offence as defined in article 69 paragraph 1 DCCP, has been met, a second criterion has to be fulfilled: the suspicion should be that a 'serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order' has been committed. This prerequisite constitutes the embedded criterion of proportionality. The criminal offence a person is suspected of has to constitute a serious breach of law and order, either by its nature or in relation to other serious offences committed by the suspect. The legislator explained that crimes like committing murder, dealing drugs and committing serious acts of fraud are in their *na-*

---

202 Which degree of suspicion can warrant the use of special investigative measures in cases of (potential) terrorist acts, see section I.A.1.b.bb.

203 "Redelijk vermoeden van schuld aan een strafbaar feit."

204 Provision 27 DCCP.

205 "Grote mate van waarschijnlijkheid dat een verdachte een strafbaar feit heeft begaan."

206 Article 326 DCC.

207 Article 321 DCC.

208 Article 285(1) DCC.

209 See also van Buiten 2016, s. 5.1.

ture crimes that constitute a serious breach of law and order. But other crimes, which are not necessarily such crimes by nature, can still constitute such a serious breach in relationship with other crimes: for example, committing forgery can result in a serious infringement on law and order when this act takes place in connection with the bribing of civil servants, according to the legislator.[210] Although the DCCP contains no explicit rule that the potential or likely sentencing range serves as a limiting criterion, the punishability of a criminal offence does play a part in the assessment of the applicability of an interception warrant via this criterion.[211]

d) Principle of subsidiarity

The third substantive prerequisite stipulates that the use of an interception measure must be urgently required by the investigation, which is an embodiment of the subsidiarity criterion. It states that an interception measure should only be used if it cannot be expected that the same investigative result will be achieved with the use of less infringing investigative measures.[212] It forms a weighted subsidiarity test, as a normal subsidiarity test will only require the use of a measure to be best suited for the purpose it is deployed for. Regarding the criterion of 'urgently requiring' it must be emphasised that no other lighter measures can or will produce the desired result.[213] However, it is not required that those other, lighter measures were actually deployed to prove that the desired result could not be obtained that way; the expectation that only an interception order will serve the purpose, suffices.

e) Persons and connections under surveillance

Although one of the recommendations of the Parliamentary Inquiry Commission,[214] in its damning report on the Dutch criminal investigation system, was that the use of interception measures should only be directed at communications in which a suspect presumably participates, this condition was not adopted in the legislative body on special investigative measures. However, this was compensated for by the decision to tighten the categories of offences for which the interception order is permitted.[215] As is the case with other special investigative measures (except for pseudo-purchase or -service), the use of those measures can be directed towards persons other than the suspect, as long as the use of the interception measure is necessary for the investigation. As the requirements for the deployment of an interception measure also apply for intercepting non-suspects, a thorough explana-

---

210 Explanatory Memorandum to the SIMA, pp. 24–25.

211 See also van Buiten 2016, s. 5.2.

212 Van Buiten 2016, s. 5.4; Explanatory Memorandum to the SIMA, p. 30.

213 Van Buiten 2016, s. 5.4.

214 See section II.C.1.

215 Van der Meijde, in: *Handboek strafzaken*, s. 16.8.

tion has to be given as to why the interception of specific communications is urgently necessary[216] and proportionate, whereby it can be expected that the latter test will be of greater weight if the interception application is directed at a person other than the suspect.

The text of article 126m DCCP is shaped in such a way that – when there is a suspect of a criminal act as described above – specific *communications* can be intercepted, via (among others) a precise description of the number or other indication by means of which the individual *user* of the communication service is identified. Article 126la DCCP offers an explanation of the terminology of the chapter on research of communications via computer systems, which specifies a *user* as 'the *natural* or *legal* person who has entered into an agreement with the provider of a communication service with regard to the use of that service or who actually makes use of such a service.' As the interception has to be directed towards the number of a specific person or entity, general interception based on certain trigger words or particular communication content is not legally possible in criminal proceedings, which is not likely to change either. What is about to change, however, is the requirement that the interception has to be directed towards a *number*. In 2017[217] a bill was proposed that would amend article 126m DCCP in such a way that it would specify that an interception order cannot only be directed towards a particular number (or, e.g., IP-address) but to all numbers that are used by the specific user during the period of validity of the interception order.[218] However, this bill has not yet been passed.[219]

8. Validity of interception orders

The provision on intercepting communications stipulates that an authorization can be given for a maximum of four weeks, for which it is irrelevant whether this is under normal circumstances or in cases of emergency. A shorter period of time is also possible, and is used frequently (e.g., a few days before a search is scheduled, in order to gain insight into the daily schedule of a suspect). In the application for an authorization, the period of validity has to be provided as is formally required in paragraph 2(e) of article 126m DCCP. It is generally given by a notation of the date and time on which the validity of the authorization starts and ends.

If the interception proves useful but the validity is about to expire, an extension can be applied for by the investigating officers. The process for extending an authorization is nearly the same as for the application of a new interception authorization. However, in the extension application special emphasis is to be put on the

---

216 See Blom, *T&C Strafvordering*, article 126m DCCP, comment 8.

217 *Kamerstukken II* 2017-18, 33 747 ('Versterking presterend vermogen politie').

218 See Blom, *T&C Strafvordering*, article 126m DCCP, comment 18.

219 This report reflects legislation and case law as of January 2019.

findings that resulted from the previous interception period; the necessity and usefulness of the interception measure must be explained. Mostly, this is done by providing, within the application, an overview of the conversations that have proven to be useful for the investigation, combined with other relevant data that was gathered.

Sometimes the use of an interception measure reveals information that points towards the commission of other offences, which can be used to widen the investigation and, if it is a criminal act for which an interception authorization can be granted, to reinforce the explanation of the urgent necessity for an extension of the interception authorization. The investigating officer will use these findings to emphasise that it is urgently necessary to extend the use of the measure. If the prosecutor, and subsequently the investigating judge, agree, the prosecutor will request the extension of the deployment of the interception measure. The validity of the interception order can be prolonged indefinitely – that is, as long as it is urgently necessary for the investigation.

When the investigative judge has granted authorization for an interception order, his involvement in the deployment of the measure is over. The prosecutor is responsible for monitoring the use of the deployment by the investigating officers and the results it produces. As the processing of intercepted communication is very time-consuming and labour intensive, the balance between usefulness and costliness is generally constantly monitored. If the interception of a specific communication line proves useless just after the interception order is given (because, for example, it proves that the suspect uses this phone number for his legitimate business, whereas he uses another for dealing drugs) the investigating officers will send the prosecutor an application to request an order to cease the interception, which will be provided by the prosecutor when he shares the opinion of the investigating officers. This is also the case when the prosecutor judges the deployment of the interception order no longer urgently necessary for the investigation or when the investigation is no longer focused on criminal acts for which the interception authorization can be granted.[220]

9. Duties to record, report, and destroy

If an interception order is made use of, different obligations apply to the processing of the data, which relate in particular to the verifiability of the use of the investigative measure and the resulting official reports. The guarantees that need to be observed relate to the right of the accused to a fair treatment of his criminal case

---

[220] Para. 5 of article 126m DCCP says that para. 6 of article 126l DCCP applies accordingly, which states the prosecutor will end the use of the interception measure when he is of the opinion that the conditions are no longer met.

and the principles of due process. Non-observance of these may, in serious cases, lead to the inadmissibility of the prosecution of the suspect.

a) Verbalising duties of investigative officers

In investigating criminal offences, investigative officers are bound by the duty to report their process of truth-finding to enable the judiciary to check whether the principles of due process have been lived up to. Article 152 DCCP states that the officers who are tasked with investigating criminal acts have to state, as soon as possible, in official reports what has been done or found during their investigation, which can only be deviated from under supervision of the public prosecutor.[221] The principle of due process demands that this deviation can only take place if that which they have performed or found after their assessment, which is subject to review by the Public Prosecution Service, cannot reasonably be of importance for any decision to be taken by the court in the final examination.[222] Therefore, any findings or actions that could be of importance to the case, either in an incriminating or exculpatory way for the suspect, will have to be put in writing. If the drafting of a report is omitted because the actions or findings are deemed of no importance, it will nonetheless be necessary to provide some reporting on what actions and findings were performed; it must be possible to effectively respond to a request by the judge in the final investigation for further justification concerning that part of the investigation, according to the Supreme Court.[223]

Statements made in official reports are done on official oath[224] and should encompass an adequate and truthful representation of the findings or actions of the investigative officer(s) in question. The construction of an official report, knowing it contains inaccuracies, can constitute perjury.[225] Generally however, formal errors that are noticed in the investigation or in the official reporting on the investigation will be subject to article 359a DCCP, which states that errors that cannot be repaired but need justification (and do not have specifically mandated legal consequences) can be dealt with by the court by: 1) a penalty reduction, 2) excluding erroneous evidence, or 3) ruling the public prosecution inadmissible (which only happens in the case of serious breaches of due process).

---

221 Article 152 para. 2 DCCP.

222 Van Hoorn, *T&C Strafvordering*, article 152 DCCP, comment 3(a); HR 19 December 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996/249, m.nt. T.M. Schalken (Zwolsman); HR 5 oktober 2010, ECLI:NL:HR:2010:BL5629, *NJ* 2011/169.

223 HR 19 December 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996/249, m.nt. T.M. Schalken (Zwolsman); Van Hoorn, *T&C Strafvordering*, article 152 DCCP, comment 3(b).

224 Article 153 DCCP.

225 Article 207 DCC; Van Dartel & Hoekendijk 2016, s. 6.8.

In 2013, official reports on the use of an interception measure were seriously questioned in court. The District Court of North Holland dealt with a case[226] in which it was shown that a number of errors were made in the investigation process. In the criminal files against the defendant a number of serious flaws in the statements in official reports on the recording of intercepted conversations was observed. From this closer consideration it followed that the actual content of the conversations was not properly provided in the official reports; recordings that were empty were given content in the reports and in the reports on other recordings the discussion participants were switched or the meaning of the conversation was subjectively interpreted. "The police apparently investigated with tunnel vision and an urge to get the suspect convicted," argued the attorney, which would constitute an obvious violation of the principles of due process and article 6 ECHR. The seriousness of the violation – the violation of the principle that the content of official reports made by investigative officers should be trustworthy and truthful – resulted in a procedural defect and a serious disadvantage for the suspect. The court ruled that the mistakes were not mere misinterpretations; the wrongful statements in the reports were deliberate and were drafted with gross negligence of the rights of the defendant; therefore it resulted in a serious breach of due process for the defendant. The court ruled that the case brought forth by the public prosecutor was therefore inadmissible. Although the Court of Appeals judged[227] that the lack of due process was not so flagrant that the criminal case was inadmissible and that the case therefore had to be referred back to the lower court,[228] the defendant in the end received a considerable penalty reduction.

b) Reporting the use and results of an interception measure

The provision on interception, article 126m DCCP, stipulates that intercepted communications have to be recorded.[229] If the content of the intercepted communications is relevant for the case, either incriminatingly or exculpatorily for the suspect, it has to be written down verbatim or comprehensively[230] in official reports and the official report needs to be added to the procedural documents.[231] If official reports on the deployment of special investigative measures are not added to the procedural documents, the use of the measure in question should at least be reported in the procedural documents.[232] No provisions require reports on the progress of

---

226 Rb. Noord-Holland 20 March 2013, ECLI:NL:RBNHO:2013:BZ4987.

227 Hof Amsterdam 27 January 2015, ECLI:NL:GHAMS:2015:152, *NJFS* 2015/89.

228 Rb. Noord-Holland 29 November 2016, ECLI:NL:RBNHO:2016:9792.

229 See also Corstens/Borgers 2011, chapter XII.13, s. 'Opnemen.'

230 WODC 2012, p. 77.

231 Article 126aa DCCP; HR 7 May 1996, ECLI:NL:PHR:1996:AB9820, *NJ* 1996/687 m.nt. Schalken (Dev Sol); Kuiper 2014, s. 7.6.6.1.

232 Article 126aa para. 4 DCCP.

interception to be submitted to the (investigative) judge, but as mentioned in section C.II.13., an extension of an interception order will require a demonstration of the usefulness of the previous interception authorization, which is generally done by providing excerpts of intercepted communications in the extension application.

c) Destroying records and official reports on the use of special investigative measures

As long as a criminal investigation is ongoing, the public prosecutor will retain all official reports and other objects (insofar as these are not included in the procedural documents), from which data can be obtained that has been gathered by deploying the investigative measures:

1) observation with the aid of a technical device that registers signals (article 126g DCCP),
2) the recording of confidential communication (article 126l DCCP),
3) the recording of telecommunications (article 126m DCCP),
4) or demanding information (via a production order) about a user and the telecommunications traffic with respect to that user (articles 126n and 126na DCCP).

He will keep these at the disposal of the investigation.[233] This includes the recordings made during interception. Two months after the case has ended and all subjects involved[234] have been notified of the use of special investigative measures on them,[235] the public prosecutor will destroy said official reports and other objects.[236] However, the prosecutor can determine[237] that the data acquired with the above-mentioned special investigative measures can be used for investigations other than the one for which the measures were deployed. Furthermore, he can decide to process and store the data in police systems.[238]

10. Notification duties and remedies

In accordance with article 13 ECHR, the Dutch legislator created a codified notification duty, which mandates the notification of those who were subjected to the use of certain[239] special investigative measures.[240] This duty, which is provided

---

233 Article 126cc para. 1 DCCP.

234 Those persons subjected to the use of special investigative measures, see article 126bb DCCP.

235 In the next section, the requirements surrounding notification will be dealt with.

236 Article 126cc para. 2 DCCP.

237 Based on article 126dd DCCP.

238 Also based on article 126dd DCCP.

239 This includes the use of a communication interception measure.

240 Corstens/Borgers & Kooijmans 2018, chapter XII.27.

in article 126bb DCCP, stipulates that the persons involved have to be informed (in writing) of the use of these measures as soon as the investigation allows such – which is mostly after the investigation is completed – and only if this is reasonably possible. Notification is not necessary if the suspect will be able to acquaint himself with the measures used against him based on the case file (e.g., when he is to appear in court to be tried). In practice, it appears that the obligation to notify is not always observed.[241]

In Dutch Criminal Procedure, there is no specific provision or procedure that provides a means to complain against the unlawful use of special investigative measures. An effective remedy therefore seems absent. However, as mentioned previously, the I&S is the central authority that checks whether the formal prerequisites for the deployment of an interception measure have been met (albeit as an organ of the National Police), which it does thoroughly. As the authorization of the investigative judge is one of the formal prerequisites, and the investigative judge checks both the formal and substantive prerequisites, unlawful use of interception measures is a rarity. However, in the event that officials do conduct interceptions illegally, the consequences might be the exclusion of evidence or the inadmissibility of the case. A few examples of such penalties have been given throughout the report; more examples are hard to find in Dutch jurisprudence.

11. Confidentiality requirements

As can be seen in previous paragraphs, a lot of requests and orders can be and *are* directed towards telecommunications providers. This is generally done in secrecy since the revelation of those actions could or would undermine the goals of an investigation. The Telecommunications Act (TA), in which the cooperation duties are stipulated, contains a specific provision on secrecy. Article 13.5 TA orders public communication networks and services to maintain secrecy on data surrounding interception orders and information procurement (user and traffic data, etc) by those involved in criminal investigations (as well as those working in the intelligence community). Furthermore, the networks and services have to properly protect said data against unauthorized access. The data received from and sent to investigative officers on interception orders and information is considered a state secret,[242] of which the unauthorized exposure would be punishable through articles 98–98c (on exposure of state secrets) or 272 (on breach of (legal) confidentiality) DCC.[243] In addition to the provision in article 13.5 TA, the DCCP has its own provision on secrecy for those who receive a production order by investigative officers. Article 126bb DCCP states that those who receive a request from the au-

---

241 WODC 2004.

242 *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 9; Koops 2005, s. 2.7.1.

243 Van der Laan & Newitt 2014, s. 5.

thorities are to observe confidentiality in the interest of the investigation and with respect to everything they know about the request. The reasoning behind this provision is stated in the explanatory memorandum: it is in the interest of the investigation that the client is not informed about the application of the powers, and the duty of confidentiality applies if the interest of the investigation requires such confidentiality.[244] Breach of this legal provision would, again, be punishable based on article 272 DCC. Next to the reactive measures mentioned above, a few general preventative provisions – directed towards the networks and providers – are given in lower legislation related to the TA. Article 2 of the Decree on Telecommunications Data Security[245] (DTDS) mandates that providers are to implement the necessary security measures to prevent unauthorized data access regarding interception and production orders, and focus on 1) measures towards personnel of the provider, 2) access to buildings and areas on which the data and information is present, 3) proper functioning and security of the information system in which the data and information are processed, 4) preventing, establishing and investigating any unauthorized violation of the confidentiality of the data and information, and 5) in the event of calamities. The Appendix to the DTDS provides further, more specific rules on how integrity and reliability of the materials obtained is to be guaranteed, among which is the instruction that 'documents in which, or interchangeable data carriers on which, the information and data are recorded, are stored in properly secured storage media.'[246]

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

a) Overview

It was already briefly mentioned above that two provisions in the DCCP provide the possibilities and safeguards on requesting traffic and subscriber data from communications providers by investigative officers. Article 126n DCCP provides the framework surrounding the request for traffic data, whereas article 126na DCCP provides the framework for requesting subscriber data from a communications provider.[247] The respective provisions are given in English below.

---

[244] *Kamerstukken II* 2001/02, 28 353, nr. 3, p. 15; Van der Laan & Newitt 2014, s. 4.1.

[245] See Appendix.

[246] Appendix to the DTDS, provision III, para. F.

[247] Article 126nc DCCP deals with using production orders for requesting identifying data from entities other than communications providers.

b) Provisions

Article 126n DCCP

1. In the case of suspicion of a serious offence as defined in section 67(1), the public prosecutor may, in the interest of the investigation, request the provision of data on a user of a communication service and the communication traffic data pertaining to that user. The request may only relate to data designated by Governmental Decree and may involve data which:

a. was processed at the time of the request, or

b. is processed after the time of the request.

2. The request, referred to in subsection (1), may be directed to any provider of a communication service. Section 96a(3) shall apply mutatis mutandis. If the request referred to in the first paragraph relates to a person who has a right to source protection, this request can only be done after written authorization, on request of the public prosecutor, by the examining magistrate. Article 218a, second paragraph, shall apply mutatis mutandis.

3. If the request relates to data as referred to in subsection (1, second sentence) (b), the request shall be made for a period of maximally three months.

4. The public prosecutor shall have an official record of the request prepared, which shall state:

a. the serious offence and if known, the name or otherwise the most precise description possible of the suspect;

b. the facts or circumstances which show that the conditions, referred to in subsection (1), have been met;

c. if known, the name or otherwise the most precise description possible of the person about whom data is requested;

d. the data requested;

e. if the request relates to data as referred to in subsection (1, second sentence)(b), the period to which the request relates.

5. If the request relates to data referred to in subsection (1, second sentence) (b), the request shall be terminated as soon as the conditions, referred to in subsection (1, first sentence), are no longer met. The public prosecutor shall have an official record made of amendment, supplementation, extension or cancellation of the request.

6. Rules pertaining to the manner in which the public prosecutor requests data may be set by Governmental Decree.[248]

Article 126na DCCP

1. In the case of suspicion of a serious offence, the investigating officer may, in the interest of the investigation, request the provision of data pertaining to name, address, postal code, town, number and type of service of a user of a communication service. Section 126n(2) shall apply.

---

[248] Translation provided by the European Judicial Training Network, http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf. The translation has been edited to match the contemporary provision in the DCCP.

2. If the data, referred to in subsection (1), is not known to the provider and is necessary for the application of section 126m or section 126n, the public prosecutor may, in the interest of the investigation, request the provider to retrieve and provide the requested data in a manner to be determined by Governmental Decree.

3. In the case of a request, as referred to in subsection (1) or (2), section 126n(4)(a)(b)(c) and (d) shall apply mutatis mutandis and section 126bb shall not apply.

4. Rules pertaining to the manner in which the investigating officer or the public prosecutor will request the data may be set by or pursuant to Governmental Decree.[249]

c) Traffic data

As can be seen in the English translation of article 126n DCCP above, several safeguards prevent the uncontrolled gathering of traffic data in criminal procedure. First off, the measure can only be deployed if a person is suspected of a serious crime as defined in article 67 DCCP (for which pre-trial detention is applicable).[250] If this is the case, the public prosecutor can, if such is in the interest of the investigation, demand via a production order that data on a subscriber/user of a communications service and data on that user's communications traffic are to be surrendered. Only data that has been processed or will be processed after the production order can be subject to such a production order and, based on paragraph 2 of the provision, the production order can be directed at any communications provider. In the production order it has to be specified 1) the criminal act and the person being investigated, 2) the facts or circumstances showing that the subjective prerequisites are fulfilled, 3) if known, the name or otherwise the most accurate indication possible of the person about whom information is demanded, 4) the data that is required, and 5) if the claim concerns data that still has to be processed (future data), the timeframe in which the claim is valid, with a maximum of 3 months.[251] If the production order concerns future data, the measure has to be terminated as soon as it becomes known that the substantive prerequisites are no longer met.[252] If the application for the production order contains all the relevant information that is required for the lawful use of a traffic data measure, the official production order can be formalised, after which it will be sent to the communications provider directly. Within the period of time mentioned in the production order, the provider will then have to deliver what is requested, which will be directly sent to the investigative officers.

---

[249] Translation provided by the European Judicial Training Network, http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf. The translation has been edited to match the contemporary provision in the DCCP.

[250] See sections III.B.7. and I.A.1.b.cc. for further information on pre-trial detention criminal acts.

[251] Article 126n para. 3 DCCP.

[252] Article 126n para. 5 DCCP.

d) Subscriber data

According to article 126na DCCP, an investigating officer may, in the event of suspicion of a crime and in the interests of the investigation, request a communications provider to provide information concerning the name, address, postcode, place of residence, number and type of service of a user of its communication service. If the aforementioned data is not (yet) known by the provider, the investigative officer can request that the provider *retrieve* and subsequently provide the requested data.[253] In practice, user data concerning a user of a communication service is requested through the Central Information Desk for Research on Telecommunications (CIOT),[254] for which each police unit has a special computer with which only authorized investigators can gain access to the CIOT-system. With this system, the data – which is mandatorily[255] updated every 24 hours by the communications services – can be consulted fully automatically.[256] The providers of internet services are to know who the user is behind a dynamic IP address and will be able to provide information that is requested by investigative officers.[257]

e) Data retention

Within the Telecommunications Act there is a specific provision concerning the mandatory retention of data by communications providers. Article 13.2a TA stipulates that public communications network or service providers shall retain the data that is generated or processed in light of the use of the offered networks or services, for the purpose of investigating, detecting and prosecuting serious crimes. This data has to be retained for 12 months if the data concerns telephone communications via fixed or mobile networks, or 6 months if the data concerns internet access, email or VoIP. The Appendix to article 13.2a TA provides what is regarded as data concerning internet access, email or VoIP in light of this provision: traffic data, the user-ID, the phone number, the name and the address of the IP-user, the log-in and log-off time of an internet session, etc. However, in 2014 the EU data retention Directive was declared invalid[258] by the EU Court of Justice, because the obligations of this directive are incompatible with the right to privacy and the right to the protection of personal data, which in turn led to a Dutch provision judge declaring the

---

253 Article 126na para. 2 DCCP.

254 CIOT is part of the Ministry of Justice and Security and is the link between investigation services and telecom companies and is responsible for the storage and use of identifying data: WODC 2012, p. 12.

255 Every 24 hours, a provider has to provide a digital file containing the up-to-date data on its subscribers: article 4, para. 2 Decree on telecommunications provision (see Appendix).

256 Blom, *T&C Strafvordering*, article 126n DCCP, comment 7.

257 Some providers can connect an internet tap on the basis of a name, address and place of residence: WODC 2012, s. 4.4.

258 EU CoJ, *Digital Rights Ireland & Seitlinger*, 8 April 2014, C-293/12 & C-594/12.

Dutch Data Retention Act[259] invalid.[260] Currently (2019) a Bill[261] is pending which would replace the current framework on data retention, but it is unclear when and if the bill might be approved. Irrespective of this, traffic and subscriber/user data can still be requested via a production order; the results of the deployment of production orders regarding this data do not seem to have changed due to the ruling of the EU CoJ or the verdict of the provision judge. Data is no longer mandatorily stored, but still retained by communications services in the interest of their own business operations, which subsequently means that this data can still be requested by the investigating officers. Whether the providers retain this data as long as they would have when the Directive was still valid is unclear and will probably vary between providers.

2. Identification of device ID (IMEI) and card number (IMSI)

As can be seen in the text of article 126nb DCCP below, a public prosecutor can order that by 'means of equipment' the number of a user of a communication service can be identified, in order to be able to subsequently deploy an interception measure or to produce a production order on traffic data. The means of equipment used is generally referred to as an IMSI-catcher, which can be deployed by specially assigned police officers. Based on this provision, an IMSI-catcher can only be used to retrieve a user's communications number and device ID – not to retrieve that user's location details (as was mentioned above in section II.C.1.).

Article 126nb DCCP

1. In order to be able to apply section 126m or section 126n, the public prosecutor may, subject to section 3.22(1)&(4) of the Telecommunications Act, order that the number by which the user of a communication service can be identified will be obtained by means of equipment referred to in that section.

2. The warrant shall be issued to a civil servant as referred to in section 3.22(4) of the Telecommunications Act and shall be in writing. In the case of urgent necessity the warrant may be issued verbally. In that case the public prosecutor shall put the warrant in writing within three days.

3. The warrant shall be issued for a period of maximally one week and shall state:
   a. the facts or circumstances which show that the conditions for the application of section 126m or section 126n have been met and
   b. the name or the most precise description possible of the user of a communication service whose number has to be obtained.

4. The public prosecutor shall have others destroy, in his presence, the official records or other objects, from which information can be derived that was obtained through ap-

---

[259] See Appendix.

[260] Rb. Den Haag 11 March 2015, ECLI:NL:RBDHA:2015:2498.

[261] Bill to Amend the Telecommunications Act with regard to the retention duty of telecommunications data, see Appendix.

plication of subsection (1), if that information is not used for the purpose of application of section 126m or section 126n.

D. Access to (Temporarily) Stored Communication Data

1. Online search with the help of remote forensic software

Since 2013,[262] there has been a lot of debate in Dutch politics on whether or not a provision should be included in the DCCP that regulates the use of a hacking measure – remotely and covertly accessing computer systems – in criminal proceedings. On 26th June 2018 the Computer Crime Act III[263] was passed, in which the definitive framework has been given for secretly penetrating a computer system as a special investigative measure. The Act will (likely)[264] enter into force during the course of 2019[265] and will add a hacking provision – article 126nba DCCP[266] – to the framework regarding special investigative measures.

a) Overview

The new provision on 'hacking by the police' will allow a (specialist[267]) investigative officer to penetrate a computer system that is used by a suspect – if necessary by technical means. He can only do so if a pre-trial detention crime[268] is investigated that – in view of its nature or its connection with other crimes committed by the suspect – constitutes a serious infringement of the rule of law, and only if the investigation urgently requires the use of the measure. If such is the case, the method can be deployed to:

a) identify certain characteristics of the computer system or the user, such as its identity or location, and the recording thereof,
b) to execute an order as referred to in Articles 126l DCCP (on interception of private communications) or 126m DCCP (on the interception of telecommunications), or
c) to execute an observation measure, whereby the public prosecutor can determine that a technical aid is attached to a person.

---

[262] In this year, a first draft of a bill was proposed that, among others, encompassed a provision on hacking. See: Muijen 2016, s. 1.

[263] Computer Crimes Act III.

[264] The entry into force has been postponed as of January 2019.

[265] Custers 2018, s. 'Wet computercriminaliteit III (2018).'

[266] The text of the new provision on hacking can be found in the text of the Computer Crimes ACT III, see Appendix.

[267] Article 126nba para. 8 DCCP.

[268] See section I.A.1.b.cc.

If the above-mentioned substantive prerequisites are met and a criminal act is investigated for which a maximum prison sentence of at least 8 years is given,[269] the hacking measure can also be used:

d) to investigate the recording of data stored in the computer system or data that will be stored during the period of validity of the order, to the extent reasonably necessary to bring the truth to light, or

e) to render data inaccessible.[270]

To deploy the hacking measure an investigative officer can send an application to the public prosecutor, who in turn will have to receive prior authorization from a Central Review Committee (CTC)[271] and the Attorney General's Office,[272] before he can request an authorization from the investigative judge.[273] If all authorizations have been received, the prosecutor can order the use of the hacking measure.

In addition to the regular formal requirements, the written documents have to encompass:

1) an indication of the nature and functionality of the technical device that is to be used for the execution of the order,[274]

2) which of the five purposes of the use of the measure given above is/are the reason(s) for deploying the measure, and – in case those purposes are either a), b) and/or c) – a clear description of the (investigative) actions to be performed,

3) with regard to which part of the automated work and which category of data the order is given, and

4) in case a technical aid is to be attached to a person, a notification of the intention to do so.[275]

The maximum period of validity of a hacking order will be 4 weeks, but they can be extended under the same conditions as other special investigative measures capable of gravely infringing rights like intercepting (tele)communications.[276] After the termination of the deployment of the hacking measure, the person affected (generally the suspect) will have to be notified of the use of the measure. The duty

---

269 Or other specially designated criminal acts, given in a 'general administrative order' ['Algemene maatregel van bestuur'].

270 Article 126nba DCCP para. 1 subs a–e.

271 'Centrale Toetsingscommissie;' it is comprised of (senior) members of the Public Prosecutors Office and the National Police and advises the Attorney General's Office on the deployment of a few of the potentially gravely infringing investigative measures, of which the hacking measure will be one.

272 'College van procureurs-generaal.'

273 See Explanatory Memorandum to the Computer Crimes Act III, s. 2.6.

274 Article 126nba para. 2 sub d DCCP.

275 Article 126nba para. 2 subs d, e, f and h DCCP, respectively.

276 Article 126nba para. 5 DCCP.

of notification will be based on the general clause 126bb DCCP.[277] If possible, the technical means used to execute the order has to be removed from the penetrated computer system after the order has been terminated. If this is not (entirely) possible and the (remaining parts of the) technical means might pose a risk to the functionality of the computer system, the prosecutor will have to inform the administrator of the computer system of this and provide the necessary information that is needed for complete removal of the technical means.[278] Furthermore, these technical means – the software used in the execution of the measure – will be subject to specific requirements which will be provided in a general decree on requirements for technical tools in criminal procedure.[279]

b) Current practice

In practice, the introduction of the hacking measure will provide various new possibilities for criminal investigations. The use of existing interception measures, such as the use of a telephone-, internet- or mail-tap, is increasingly impacted by both jurisdictional issues and encryption methods, which also impact the use of search and seizure measures.[280] The measure in article 126nba DCCP will allow the use of spyware (or 'policeware') and will potentially provide the opportunity to remotely and covertly turn on cameras, microphones and GPS, record keystrokes by keyloggers, make screenshots and search data (including stored or draft communications data[281]) stored on computer systems.[282] This means that data can be obtained before it is encrypted for storage on the computer system or for transmission, and could therefore be used to listen in on suspects using encrypted communications/VoIP channels,[283] such as Skype. Furthermore, passwords can be retrieved as well, so that the encryption can be undone afterwards.

For years, police services struggled with the absence of a remote hacking measure, as the existing range of investigative measures did not offer adequate solutions to these new developments. Although the measure of article 126l DCCP warrants the (covert) bugging of confined spaces (including homes) and also warrants the

---

277 See section III.B.10.

278 Article 126nba para. 6 DCCP.

279 Decree on technical means in criminal procedure (Besluit technische hulpmiddelen strafvordering).

280 Oerlemans 2017, s. 3.2.1 & 2.

281 Explanatory Memorandum to the Computer Crimes Act III, s. 2.3.2., p. 20.

282 Custers 2018, s. 'Strafprocesrechtelijke onderdelen;' Oerlemans 2017, s. 3.2; Computer Crimes Act III, pp. 19–25.

283 Explanatory Memorandum to the Computer Crimes Act III., s. 2.3.4. Also Muijen 2016, s. 3.4.

use of hardware (and, debatably, software)[284] keyloggers or even the physical breaking into a suspect's computer to install interception software,[285] the use of said measure comes with serious disadvantages; the possibility to place a bug by means of software that is placed on the computer remotely, i.e., *online* is not provided for. The need to physically access the location of the computer system is a major obstacle as the location of the automated work is not always known. Furthermore, in cases where the location *is* known, there might be a serious chance of discovery or unforeseen circumstances that could jeopardise the investigation.[286] A third shortcoming of the use of this provision is that the use of the measure requires a focus on intercepting *communications*. It cannot be used to gather data that is entered into the computer for storage or personal use. The Koops Committee signalled this problem, as well as – more generally – the fact that within the DCCP and in relation to the DCC, the definition of 'communication' differs between the various provisions. The Committee therefore advised the legislator to implement a broad definition of what constitutes 'communications,' which should be 'any data transfer between persons or machines.' This would include 'self-communications' (i.e., the entering of data into a computer for storage on the device) and the communications between machines (regarding the Internet of Things).[287]

Furthermore, the new provision entails that jurisdictional problems can be circumvented, as data can be obtained before transmission across the border. This would normally require foreign legal assistance, which is often time-consuming, costly and does not always succeed. Regarding jurisdictional issues, the explanatory memorandum also provides some considerations that are potentially far-reaching; if the suspect or the evidence linked to him cannot be localized, for instance because cloud computing services or anonymization techniques are being used, the hacking measure can also be used extraterritorially.[288] As soon as clarity has been gained on the location of the suspect or the evidence during the deployment of the measure, the foreign authorities have to be informed of the use of the measure on their territory.[289]

---

[284] The explanatory memorandum of the Special Investigative Measures Act specifically mentions hardware keyloggers, which can be used on computers that are connected to a network (as the measure should only be used to intercept communications): Explanatory Memorandum of the the Special Investigative Measures Act, p. 35.

[285] Koops 2014, s. 4.2; Koops & Buruma 2007; Oerlemans 2011, s. 6.1.1.

[286] Explanatory Memorandum to the Computer Crimes Act III., s. 2.1.3 "cloudcomputingdiensten."

[287] Koops Committee Report 2018, s. 6.3.1. An English version of the summary will be published in the course of 2019.

[288] If it is known beforehand that the use of the measure might partially take place in another jurisdiction, the (formal documents for acquiring a) hacking authorization will have to mention this, so that the investigative judge can include this in his judgment.

[289] Explanatory Memorandum to the Computer Crimes Act III., s. 2.8.3; Oerlemans 2017, s. 3.2.2.

2. Search and seizure of stored electronic communication data

It is not only during covert operations, but also during overt operations such as searches, that data can be acquired in the interest of an investigation. As Dutch doctrine does not allow for data to be seized (only tangible objects[290] – 'goods' – can be seized, such as data carriers), this has resulted in the problem that searches could not be executed just to acquire data. A second issue surrounding the seizure of data is that the seizing of a data carrier is not always proportionate or feasible in practice.[291] To tackle both problems, in 2005 the legislator introduced a provision in the section of the DCCP on search and seizure – article 125i DCCP – to deal with this issue.[292] The provision allows for the search of a place to *secure*[293] data that is stored or fixed on a data carrier in that location. The definition is fairly broad: a data carrier can be a computer, but also a USB stick or even paper. Article 125j DCCP is also important in this respect: it provides the opportunity to perform a network search during the search of a place and entails that a computer system located elsewhere can be remotely searched during the search of the initial place. This is to be distinguished from a remote, *covert* search, which is not yet permitted in Dutch criminal procedure.[294] A network search can only be performed if the connection to the remote computer is lawfully accessible to people regularly living, working, or staying at the searched location.[295] The measure is further limited by the fact that: 1) it can only be performed within Dutch territory, 2) the network search can only be performed from the location of the search and not after the computer has been seized (the network search cannot be continued after the seized computer is brought to a police station) and 3) it cannot be performed on a computer that is encountered outside the situation of a search (e.g., during the apprehension of a suspect in public).[296]

This framework does however provide the opportunity to gather communications data other than by using the measures[297] on interception of communications data, which focus on data 'in transit.' Stored communications data is, in contrast to communications data in transit, not protected by the constitutional protection of

---

290 An exception to this is the seizure of electronic money, such as crypto-currencies.

291 Koops, s. 3.6.6.

292 Data Production Order Act; Koops 2016, s. 3.6.6.

293 'vastleggen.'

294 See previous subsections.

295 Koops 2016, s. 3.6.7.

296 Van Dijk & Keltjens 1995, p. 235-236; Koops, Conings & Verbruggen 2016, p. 38; Koops 2016, s. 3.6.7. The strict interpretation as to what constitutes a network search might be considerably loosened, as the Koops Committee warned the legislator that the current framework is increasingly limiting the adequate investigating of computer systems; more and more data is stored in the cloud, which makes network searches more time-consuming.

297 Articles 126m and 126l DCCP.

article 13 DC.[298] Therefore, the gathering of this data does not require the involvement of an investigative judge.[299] Furthermore, there is no specific *lex specialis*-relationship between using measures on stored communications data or the measures on intercepting communications data; if both can be used, one is not to be chosen over the other. These observations entail that the gathering of stored communications data is subject to a significantly lower threshold.

In addition to the possibilities of gathering communications data via production orders directed at communications providers[300] or others who are (thought to be) in possession of said data,[301] stored communications data can also be encountered during a search. This data can be investigated and secured like any other data and is not specially protected, except when the search is conducted at a communications provider (as the data is then considered to be in transit).[302] In this latter case – when the provider has the power of disposal of the data – the data can only be investigated or secured on authority of an investigative judge and only if the suspect is the sender, receiver or subject of the data, or if the crime is committed with said data.[303]

3. Duties to cooperate: production order and decryption order

Several provisions on the search and seizure and interception of data within the DCCP provide cooperation duties for third parties. Most prominently described in this report is the cooperation with communication network and service providers, based on article 126m DCCP and other provisions. As mentioned above, encryption poses a growing problem for criminal investigations, not just because of tech-savvy criminals who use the latest in technology in their efforts to avoid apprehension, but also because of the increase in encrypted communications offered to the general public. Regarding both problems the legislator has implemented provisions on production and decryption orders, in an effort to tackle its impact. These will be discussed below.

a) Produce and decrypt in the interception via communications providers

Paragraph 6 of the provision on interception via communications providers, **article 126m DCCP**, states that:

---

298 This constitutional provision protects the secrecy of mediated communications entrusted to transport providers; this only applies to telephony, but the legislator has generously considered it to also usually apply to (confidential) electronic communications): Koops 2016, s. 4.5.5.2.

299 Although there are a few exceptions, for instance regarding data concerning communications with medical specialists, attorneys, etc.

300 Article 126ng DCCP.

301 Article 126nd DCCP.

302 Koops 2016, s. 4.5.5.2.

303 Article 125la DCCP; Koops 2016, s. 4.5.5.2.

> Insofar as is specifically required in the interest of the investigation, the person, who may be reasonably presumed to have knowledge of the manner of encryption of the communications, may be requested, if subsection (1) is applied, to assist in decrypting the data by either providing this knowledge, or undoing the encryption.[304]

Chapter 13 of the Telecommunications Act stipulates that communications providers can only make their networks and services available to the public if these can be intercepted if necessary.[305] They must therefore be able to undo any encryption that they have applied. However, this duty – to provide decrypted access to data communications or to provide the necessary passwords – does not offer help in all cases. Communications services can also be provided by non-national providers, who are generally not bound by these national regulations. Furthermore, internet service providers are not always able to undo the encryption of data that runs via their networks, as this data might have been encrypted by intermediate services who are not bound by the Telecommunications Act or the decryption order of article 126m paragraph 6 DCCP.[306]

b) Produce and decrypt in the execution of production orders

Article 126nh DCCP[307] was introduced in 2006 to make sure that the execution of a production order based on articles 126nd (regarding historical content data), 126ne (regarding future content data) or 126nf (regarding sensitive data) DCCP results in useful and decrypted data.[308] This provision stipulates that the public prosecutor can order a person (not being a suspect), who is reasonably presumed to have knowledge of the method of encryption of the data targeted in the production order provisions in question, to cooperate in decrypting this data by actually decrypting it or by providing the knowledge to do so. Failure to comply with this duty will result in a breach of article 184 DCC, which incriminates those who refuse to comply with an order or production order of an officer in an official capacity, such as an investigating officer or a public prosecutor. This refusal is punishable with up to 3 months imprisonment.[309]

---

304 Paragraph 7 of this provision further states that the production order of paragraph 6 cannot be given towards suspects.

305 Article 13.1. para. 1 TA.

306 Oerlemans 2012, p. 29.

307 The articles 126uh and 126zg DCCP provide similar duties for these production orders in the context of investigations into crimes committed or planned in an organised context or terrorist acts.

308 Data Production Order Act.

309 Maessen, *Handboek Strafzaken*, s. 15.7.2.

c) Produce and decrypt – search and seizure

The provision on the decryption duty regarding production orders above, was based on article 125k DCCP that provides similar duties regarding data seized during searches:

> **Article 125k DCCP**
>
> 1. Insofar as is specifically required in the interest of the investigation, the person who may be reasonably believed to have knowledge of the security system of a computerised device or system may be ordered, if section 125i or section 125j is applied, to provide access to the computerised devices or systems present or parts thereof. The person who is ordered to do so must comply with this order, if requested, by providing the knowledge about the security system.
>
> 2. Subsection (1) shall apply mutatis mutandis if encrypted data is found in a computerised device or system. The order shall be directed to the person who may be reasonably believed to have knowledge of the manner of encryption of this data.
>
> 3. The order, referred to in subsection (1), shall not be given to the suspect. Section 96a(3) shall apply mutatis mutandis.[310]

As can be seen, the provision specifically aims at supporting the measures of articles 125i and 125j DCCP, which were dealt with extensively in previous sections. When a computer is searched during the search of a place, or when a network search is performed from that place, a person who is reasonably assumed to have knowledge of the method of security of a computer system, can be ordered to grant access or provide information on how to access said system. Again, failure to comply with this duty will result in a breach of article 184 DCC.

d) Nemo tenetur

Paragraph 3 of article 125k DCCP, which is provided in the previous subsection, mentions that an order to provide access to a computer system during a search cannot be directed towards the suspect. However, this is not only a specific prohibition under article 125k DCCP, but is built into paragraph 2 of article 126nh DCCP[311] as well, and stems from the privilege against self-incrimination ('nemo tenetur'). Although overthrowing this principle was considered during the drawing up of the Computer Crimes Act III,[312] it is still forbidden to force a suspect to (provide information on how to) access encrypted or secured computer systems or data. The prohibition was formulated in light of article 6 ECHR and has been a long-standing doctrine in Dutch criminal procedure. The ECtHR case of *Saunders v. the United Kingdom* further strengthened the Dutch interpretation that a suspect does not have

---

310 Translation provided by the European Judicial Training Network, http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf. The translation has been edited to match the contemporary provision in the DCCP.

311 General provision regarding decryption and the use of productions orders.

312 Bood 2018, s. 1.

to contribute to his own conviction and therefore has the right to remain silent.[313] Therefore, he cannot be forced to provide information that 'exists dependent on his will,' such as passwords and encryption keys (that are not written down).[314] What is currently in debate, is whether biometric-based security measures (rather than password-based ones) are protected by the *nemo tenetur*-principle; a lot of devices (can) require a fingerprint to grant access to the data on the device. Biometrics exist independent of the will of the suspect.[315] Koops *et al*. argue that a coercive power could be adopted in the DCCP that provides the basis for an order to unlock a device that is biometrically protected, which for suspects and non-suspects entails a *duty to tolerate* their fingerprints being used to unlock devices – if necessary by force.[316]

IV. Use of Electronic Communication Data in Court Proceedings

1. Regulations on the use of interception evidence in court proceedings

As mentioned in the paragraph on recording and reporting duties,[317] the recordings of communications gathered with the use of an interception measure are transcribed in official reports, either verbatim[318] or comprehensively, after which the reports are added to the case file.[319] The public prosecutor is responsible for compiling the case file and has to ensure that any evidence relevant for either the court or the defence is present, based on which they can oversee the complete investigative process that took place, as well as the legitimacy of the gathered evidence.[320] The recordings themselves are not (automatically) added to the case file, but can be if the public prosecutor deems this necessary or desirable. The prosecutor can also do so on request of the defence[321] or the court. As a general rule, any evidence that is incriminating or exculpatory for the suspect cannot be withheld from him. Transparency of the investigative process is key and substantiated requests to in-

313 For further discussions on this issue, see Koops 2012b.

314 Of course, passwords that are found during a search can be used by the investigative officers.

315 A recently published verdict of the lower court of North-Holland states that the court is of the opinion that such action does not violate the principle of nemo tenetur: Rb. Noord-Holland 14 December 2018, ECLI:NL:RBNHO:2018:11578.

316 Commissie Koops, s. 5.5.2; disagreeing: Bood 2018.

317 Section III.B.9.

318 In case they are relevant for the investigation: WODC 2012, s. 4.5.2.

319 WODC 2012, s. 6.9, pp. 77 and 117.

320 Designation on investigative powers 2011, s. 5.2.

321 WODC 2012, s. 6.9, pp. 77 and 117.

spect the validity and integrity of the investigations' findings must be honoured. This means that (a copy of) the recordings based on which official reports are composed, can be requested to test the validity of the reports – as is the case for information on the technical execution of the interception measures used (whether such a request would be granted is debatable, as the technical execution of interception is standardized). Generally, recordings are not part of a case file, nor are there specific rules for using intercepted electronic communication data. However, as already explained in the paragraph on recording and reporting duties, the transcripts that are presented in official reports have to be representative of the communications that have been intercepted, whereby grave deviations can potentially lead to exclusion of this evidence or even the inadmissibility of a case,[322] although this rarely happens.

2. Digital data as evidence

As the digitization of society progresses, Dutch criminal cases increasingly contain digital evidence which poses new problems – especially regarding integrity and verifiability in court proceedings. General practice regarding seized data carriers is to create an image of the (complete) digital content of these devices, and/or assign a hash value to the data. This allows investigative officers to examine the data without (accidentally) altering it, therefore retaining the integrity of the evidence. Furthermore, it allows the other parties involved in criminal procedures – the courts and defence – to verify the findings of the prosecution.[323]

3. Data obtained about other offences and other suspects

During the use of an interception measure, communications data can be gathered that points towards other criminal acts committed by the suspect, or by subjects other than the suspect. Although an interception measure is acquired based on a certain suspicion and against a certain individual, this does not mean that the evidence gathered using said specific measure cannot be used for other purposes. Or, as Corstens and Borgers put it, the investigative officers do not have to close their ears to additional information.[324] Based on article 126dd DCCP the information can be used for purposes other than the investigation for which the measure was deployed – either the prosecution of other criminal acts, or investigating and prose-

---

[322] For example, Rb. Zutphen 7 October 2009, ECLI:NL:RBZUT:2009:BJ9577: in this case it seemed to the court that interception transcripts were gravely inaccurate, possibly on purpose, and therefore ruled the case was inadmissible. See also Buruma 2008.

[323] For further reading on this subject, see Koops & Oerlemans 2019, s. 3.10.

[324] Corstens/Borgers 2011, chapter XII.13, s. 'gebruik tegen derden,' *referring to Supreme Court-case (Conclusion)*: HR 10 January 1984, ECLI:NL:PHR:1984:AC1211, m.nt. Th.W. van Veen.

cuting other suspects. Of course, deploying an interception measure based on a certain suspicion solely to gather evidence regarding a crime for which an interception authorization cannot be acquired, would constitute abuse of power and is impermissible.[325]

4. Data obtained from intelligence services

The Dutch Supreme Court specified in 2006 that information gathered by Dutch intelligence services can be used to start a criminal investigation and said information can be used as evidence against suspects. The use of interception records from these intelligence services is not excluded.[326] As far as such use is concerned, it must be noted that the criminal judge will have to assess with caution, on a case by case basis, whether the material can be used as evidence; such information cannot always be fully tested on reliability due to the (statutory) secrecy surrounding intelligence operations and the origin of obtained materials or knowledge.

5. Data obtained from foreign jurisdictions

Evidence that is gathered by foreign authorities can be used in Dutch court proceedings. Investigating the legality of the acquisition of said evidence is only necessary if there are substantial indications that it has been acquired in violation of the applicable law in the country of origin (principle of legitimate expectation)[327] and the usage of the evidence must further be tested on its compatibility with article 6 ECHR.[328] The treatment of evidence that originates from non-national services, including evidence gathered by using interception measures, is basically treated equally to that of national services, and is therefore tested on reliability and legality as would be done with any other evidence.[329]

---

[325] Corstens/Borgers 2011, chapter XII.13, s. 'gebruik tegen derden.'

[326] HR 5 September 2006, ECLI:NL:HR:2006:AV4122, *NJ* 2007/336, m.nt. T.M. Schalken.

[327] HR 31 January 2016, ECLI:NL:PHR:2006:AU3446, *NJ* 2006, 365, m.nt. Reijntjes; Reintjes & Reijntjes-Wendenburg, *Handboek strafzaken*, s. 34.2.11.

[328] ECtHR, *P.V. v. Germany*, 13 July 1987, no. 11853/85; also ECtHR, *Stojkovic v. Belgium & France*, 27 October 2011, no. 25303/08, *NJ* 2013/1, m.nt. Reijntjes; Rb. Rotterdam 8 oktober 2008, ECLI:NL:RBROT:2008:BF7620, *NJFS* 2008, 239; Reintjes & Reijntjes-Wendenburg, *Handboek strafzaken*, s. 34.2.11; further Luchtman 2013, s. IV.1.1.7.2.2.

[329] Luchtman 2013, s. IV.1.1.7.2.2.

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

1. International Conventions

To assure effective cooperation in investigating and prosecuting criminal acts internationally, the Netherlands has acceded to various international and European treaties – multilaterally and bilaterally – over the past decades. These include:[330]

– *The European Convention on Mutual Assistance in Criminal Matters of 1959*, which came into force in the Netherlands on 15th May 1959. The Kingdom of the Netherlands has made reservations with regard to article 2 (grounds for refusing legal assistance requests), article 5 (concerning the execution of rogatory commissions seeking to conduct searches or seizure), article 11 (passage), article 22 (exchange of statements concerning convictions) and article 26 (application in relation to Benelux countries and other EU countries);

– *The Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000,* which came into force on 23rd August 2005. The Netherlands has made reservations with regard to article 10(9) (concerning video conferences) and assigned the International Judicial Assistance Bureau (which was later renamed the Department of International Legal Aid in Criminal Matters (AIRS)[331]) as the competent central authority within the meaning of article 6(2) & (8). The public prosecutor is the assigned authority for (the execution of) incoming and sending outgoing requests, as well as for the notification of a Member State for instituting proceedings before the courts in another Member State, and the examining magistrate for outgoing requests (article 6(5)). The competent authority within the meaning of article 18, article 19 and article 20(1) to (5) is the public prosecutor, and the competent authority to receive the notification referred to in Article 20(2) is the Netherlands Sirene Bureau;[332]

– *The United Nations Transnational Organized Crime Convention of 2000*, which came into force on 25th June 2004. Two reservations are in place: in reference to article 16 paragraph 5, under a), the Kingdom of the Netherlands declared that it will take this Convention as the legal basis for cooperation on extradition with

---

330 For an overview of all multilateral treaties concerning mutual legal assistance the Netherlands is a Party to, see Dijkstra & Verrest/Verrest, *T&C Internationaal strafrecht,* 'commentaar op Sv.'

331 'Afdeling Internationale Rechtshulp in Strafzaken,' a department within the Ministry of Justice & Security.

332 For further (less relevant) reservations made by the Netherlands concerning this Convention, see https://verdragenbank.overheid.nl/nl/Verdrag/Details/009284_b#Nederlanden,%20het%20Koninkrijk%20der.

other State parties to this Convention; in accordance with article 18 paragraph 13, the central authority is the Ministry of Justice;[333]

– *The Convention on Cybercrime*, which came into force on 1st March 2007. In accordance with article 24 paragraph 7, the authority designated by the Netherlands is the Ministry of Justice. In accordance with article 27 paragraph 2.c. of the Convention, the central authority designated by the Netherlands is the National office of the Public Prosecution Service, which is also the point of contact in accordance with article 35;

– *Directive 2014/41/EU regarding the European Investigation Order*: on 31st May 2017 a (partial) Bill was determined (regarding legal assistance in investigations), the 'Bill amending the Code of Criminal Procedure and any other laws regarding the regulation of international cooperation in criminal matters' (Revision of the regulation on international cooperation in criminal matters). On 31st June 2017 the main Bill was determined, the 'Bill to amend the Code of Criminal Procedure implementing the Directive 2014/41/EU of 3rd April 2014 concerning the European Investigation Order in criminal matters' (Implementation of the European Investigation Order Directive). The competent central authority to receive and send EIO's is the National Centre for International Legal Assistance (hereafter: LIRC) or one of the 10 regional Centres for International Legal Assistance (IRC's).[334]

2. Bilateral treaties

As the Dutch national framework on mutual legal assistance no longer requires a treaty-basis with a foreign State to execute that State's request for the use of special investigative measures,[335] the listing of bilateral treaties that would allow the use of interception measures (of which a comprehensive overview seems unavailable) seems superfluous. An important note in this regard is however, that the real-time transfer of communications data still requires a treaty basis. The only treaty, based on which States that are not a Party to the Directive (regarding the European Investigation Order) can request real-time transfer of communications, is the EU Convention on Mutual Assistance. This treaty is therefore still relevant for cooperation with Denmark and Ireland. If a foreign State is a Party to neither of these legislative bodies, the regular national framework for mutual legal assistance is applicable and the real-time transfer of communications data cannot be executed.

---

333 For the Kingdom of the Netherlands in Europe, not the Antilles. The same goes for all other mentions of a central authority based on the treaties mentioned in this section.

334 '(Landelijk) Internationaal Rechtshulp Centrum.'

335 See next section.

3. National regulation

Recently,[336] the national framework for cooperation in the execution of mutual legal assistance (MLA) has seen a significant restructuring, in which the introduction of the European Investigation Order (EIO) has been of significant importance. The restructuring has meant that there is now a separation between the acknowledgement and execution of EIO, and MLA-requests that are *not* based on the EIO. In the latter case, basic regulations apply, in which an even further division has been made between requests that are based on treaties and those that are not.[337] The provisions regarding these regulations can be found in Book 5 of the DCCP. Under the old regime, an MLA-request to deploy special investigative measures could not be granted if the request was not based on a treaty between the Netherlands and the requesting State that provided the legal means to do so. However, these restrictions have been lifted with the introduction of the Amendment of the DCCP regarding international cooperation.[338] In order to comply with *any* request for legal assistance from a foreign State, investigative powers – including the use of interception measures – may now be applied in so far as these could also be applied in Dutch investigations.[339]

B. Requirements and Procedure

1. Overview

Below, the requirements and procedure surrounding incoming and outgoing requests for legal assistance will be outlined. It is important to note that the texts given under section B.2 and B.3 refer to the national framework as implemented in the DCCP. The provisions in this framework are relevant for requests based on the 'old' system (non-treaty based or based on the EU MLA Convention) and *not* for the execution of EIO. Section C will give an examination of the framework regarding incoming and outgoing EIO, as far as the procedure differs from the regular framework in light of the execution of interception measures.

---

336 1 July 2018.

337 Explanatory Memorandum to the Amendment of the DCCP regarding international cooperation, p. 11 (see Appendix).

338 Went into force on 1st July 2018, see Appendix for references.

339 Explanatory Memorandum to the Amendment of DCCP regarding international cooperation, p. 9.

2. Incoming requests

a) Requests for the execution of investigative measures

If no treaty between the Netherlands and the foreign State stipulates otherwise, incoming requests for legal assistance will have to be sent to the AIRS by the foreign authorities. In principle, any incoming request that is not immediately deemed ungrantable by the Minister of Security and Justice will be forwarded to the public prosecutor. Insofar as an incoming request for legal assistance is based on a treaty, the desired result is granted as often as possible.[340] In that case, the content of the treaty also supersedes the national provisions as far as these frameworks are not compatible.[341] A decision to not grant an MLA-request can only be made if there are any impediments of an essential nature arising from the applicable treaty or the law (based on the grounds for refusal or if the requested investigative power cannot be applied under Dutch law), or if compliance with the MLA-request would be at odds with fundamental principles of Dutch criminal procedure.[342] Grounds for refusal to execute an MLA, as given in the national framework, are:

1. the principle of *ne bis in idem*,[343]
2. a conflict with Dutch interests of prosecution,
3. the apparent violation of fundamental rights (ECHR),
4. the suspicion that the investigation for which the request is made, intends to prosecute or punish a suspect with regards to his religious, philosophical or political conviction, nationality, race or population group, or
5. a suspicion that the criminal acts that are investigated have a political nature.[344]

It should be noted that these grounds for refusal given in the national framework only apply insofar as no treaty applies which provides its own superseding set of limitative grounds for refusal. If the public prosecutor, having received a foreign request from the AIRS, is of the opinion that the request cannot be executed, for instance because one of the grounds for refusal applies, the request will not granted.[345]

For the evaluation of a foreign request, further national regulations apply. The use of special investigative measures in light of the execution of an MLA-request

---

340 Article 5.1.4. para. 2 DCCP.

341 HR 13 January 2009, ECLI:NL:HR:2009:BF0837.

342 Verrest, *T&C Strafvordering*, article 5.1.4. DCCP, comment 4, in reference to: HR 19 March 2002, ECLI:NL:HR:2002:ZD2927, *NJ* 2002/580; HR 5 November 2013, ECLI:NL:HR:2013:1109.

343 The equivalent of double jeopardy in common law.

344 Article 5.1.5. DCCP.

345 Formally, this decision is taken by the Minister: Verrest, *T&C Strafvordering*, article 5.1.4. DCCP, comment 3.

must meet the same prerequisites as would apply in regular Dutch investigations.[346] However, two substantive prerequisites that apply nationally for the deployment of investigative measures – the criteria that the deployment must be in the interest of the investigation and that the suspicion must focus on a criminal act that constitutes a serious breach of the rule of law (proportionality) – do not apply for the execution of a foreign request that is treaty-based;[347] this would be incompatible with the requirement[348] that treaty-based requests must be executed as far as possible.[349] Furthermore, the judgement whether the deployment of the measure is in the interests of the investigation and that the criminal act seriously breached the rule of law, is up to the foreign authorities to evaluate, as it is *their* investigation, into crimes that have been committed within *their* territory.[350]

As is the case in regular Dutch investigations, the public prosecutor is the central authority for the execution of investigative measures that have been requested and granted regarding MLA.[351] If a competence or power requires the involvement of an investigative judge according to Dutch criminal procedure, said competence or power can only be applied if the request for MLA stems from, or is authorized by, judicial authorities in the foreign State.[352] After an MLA-request has been executed, the results acquired by the execution can be handed over to the foreign authorities by the public prosecutor (via the AIRS or otherwise). However, in some cases the transfer of the requested information requires the permission of the lower court. This applies to the results gathered by the use of several of the investigative measures dealt with in this report,[353] among which is the interception of communications. The review of the council chamber of the court is limited to testing whether the requirements of the treaty and the national framework have been met, such as the requirements for compliance, the possible grounds for refusal, and whether the exercise of powers by the Dutch police and judiciary was in accordance with the law and its fundamental principles.[354]

---

346 Verrest, *T&C Strafvordering*, article 5.1.4., comment 3.

347 Article 5.1.8. para. 1 DCCP.

348 Article 5.1.4. para. 1 DCCP.

349 Verrest, *T&C Strafvordering*, article 5.1.4., comment 4, in reference to HR 22 May 2012, *NJ* 2012/399.

350 Verrest, *T&C Strafvordering*, article 5.1.4., comment 4.

351 Article 5.1.6. DCCP.

352 Article 5.1.8. para. 3 DCCP.

353 Articles 126l, 126m, 126nd para. 6, 126ne para. 3, 126nf, 126ng, 126s, 126t, 126ue para. 3, 126uf and 126ug DCCP.

354 Verrest, *T&C Strafvordering*, article 5.1.10. DCCP, comment 4; Explanatory Memorandum to the Amendment of DCCP regarding international cooperation, pp. 9–10; HR 22 May 2012, ECLI:NL:HR:2012:BV9212, *NJ* 2012/399, m.nt. A.H. Klip.

b) Foreign interception regarding communications of persons in Dutch territory

In addition to requests for legal assistance in the interception of persons within Dutch territory, the national legal framework also offers the possibility for foreign States to intercept communications of persons within the territory of the Netherlands *themselves*. Article 5.1.13 DCCP provides rules for the notification by a foreign authority, which should indicate their intention that telecommunications will be intercepted from a user who is on Dutch soil. The provision was introduced in accordance with article 20 of the MLA Convention and provides the opportunity for foreign authorities to intercept the communications of a foreign communications device that enters Dutch territory, although conditions apply: there must be a treaty-based relationship with the foreign authorities who provide the legal basis for such interception and the foreign authorities are obliged to notify the Dutch authorities of their intentions. In turn, the Dutch authorities will determine swiftly whether such interception can be performed in light of national legislation regarding the interception of communications.[355] To do so, the notification will be sent by the prosecutor to the Attorney General's Office[356] and subsequently to an investigative judge accompanied by a request to grant authorization. The investigative judge will provide a decision and – if he grants authorization – will provide the maximum duration of the authorization. The public prosecutor is then tasked with sending the foreign authorities the authorization and accompanying conditions. If the investigative judge decides that he will not grant authorization, the public prosecutor will inform the foreign authorities of this without delay, after which the interception must be terminated immediately and the gathered data cannot be used; the interception data must be destroyed.[357]

3. Outgoing requests

In Book 5, Title 1, section 2 of the DCCP, the provisions are given that specifically deal with the regulations surrounding outgoing requests for legal assistance. It specifies that the public prosecutor, the investigative judge and the courts are authorized to send a request to foreign authorities regarding legal assistance.[358] The actual sending of a request is to be performed by the Ministry of Justice and Security,[359] for which the AIRS is specifically designated.[360] If the request is solely meant

---

[355] Verrest, *T&C Strafvordering*, article 5.1.13. DCCP, comment 3, referring to the explanatory memorandum of the provision.

[356] Verrest, *T&C Strafvordering*, article 5.1.13. DCCP, comment 4.

[357] Article 5.1.13. paras. 6 and 7; Verrest, *T&C Strafvordering*, article 5.1.13. DCCP, comment 6.

[358] Article 5.1.2. para. 1 DCCP.

[359] Article 5.1.2. para. 3 DCCP.

[360] Verrest, *T&C Strafvordering*, article 5.1.2. DCCP, comment 3.

to retrieve information from foreign investigative officers, a national investigative officer can also send a request himself under the authority of a public prosecutor (without intervention of the AIRS).[361] A request for legal assistance in the execution of any measures (coercive or special investigative) can only be sent if the prerequisites for the execution of the measure in question have been fulfilled as would be required in national investigations.[362] For a request to intercept communications this means that an investigative judge must have given prior authorization on request of the public prosecutor, only after which the request can be sent to a foreign State.[363]

4. Real-time transfer of communication data

The legal framework encompassed in Book 5 of the DCCP, which gives the basic structure for MLA, offers the use of a real-time transfer of communications data in article 5.1.12 DCCP, which implemented article 18 of the MLA Convention into the national framework. For the use of these means, the conditions for the use of communications interception as given in articles 126m and 126t DCCP[364] apply accordingly.[365] The same goes for the notification duties that are stipulated in article 126bb DCCP, which state that persons affected by the use of the measure should be notified as soon as the investigation allows.[366] It is important to note that a restriction is in place regarding the real-time transfer of communications data; a request for such a transfer that is *not* treaty-based, cannot be executed.[367] As the national provision is an implementation of article 18 of the MLA Convention and no other treaty provides a basis for the direct transfer of communications data, in effect only EU Member States can request the Netherlands for the execution of such a measure.[368] If a request for real-time transfer is granted, further regulations apply: if the user whose communications are intercepted is in Dutch territory, the

---

361 Article 5.1.2. para. 2 DCCP.

362 Article 5.1.3. DCCP; HR 29 September 1987, ECLI:NL:PHR:1987:AC9986, *NJ* 1988/302, m.nt. Th.W. van Veen.

363 Verrest, *T&C Strafvordering*, article 5.1.3. DCCP, comment 2.

364 The use of the interception measure in investigations based on the suspicion that serious crimes are planned or committed by a criminal organisation.

365 Although substantive assessment is not required if the request on intercepting communications is merely of a technical nature: if a person does not reside in Dutch territory but a request for technical assistance is received, the substantive prerequisites do not have to be fulfilled. See BIRS 2004, p. 26.

366 For this, the Dutch prosecutor is responsible, but whether or not the investigation allows the notification is subject to the judgement of the foreign authorities and requires alignment between both authorities, see Verrest, *T&C Strafvordering*, article 5.1.12. DCCP, comment 5;

367 Article 5.1.12. DCCP; Amendment to the DCCP regarding international cooperation, p. 6 (see Appendix).

368 See section V.A.2.

real-time transfer of communications data is subject to the conditions that 1) this cannot be used and has to be destroyed if it contains statements by or to a person subject to a privilege of non-disclosure, and 2) this can only be used for the criminal investigation for which the MLA-request was submitted, unless permission for other use has been requested and received in advance.[369] The technical execution of real-time transfer of communications data entails that I&S will connect a tap in its interception system with respect to the requested communications, and in turn will provide the foreign authorities access to the data as soon as this data is recorded.

Given this fact and based on the overview that is given above, it seems that no technical, legal or organizational reform would be needed to ensure that the Netherlands is equipped for real-time cooperation in intercepting communications on behalf of other foreign authorities, provided that these States have either acceded to the MLA Convention or the European Investigation Order Directive (see next section). Effectively, this means that cooperation in real-time transfer of communications data will be based on the 'old' scheme of the EU MLA regarding Ireland and Denmark, whereas such transfer in cooperation with any of the other EU Member States will be based on the EIO Directive. That the effectiveness of this cooperation will likely increase regarding the latter States, will be set out in the next section.

C. European Investigation Order

1. Requirements

Title 4 of the 5th Book within the DCCP implements the EIO Directive into national criminal procedure and stipulates the requirements and possibilities for mutual legal assistance between the Netherlands and other European Member States – except Ireland and Denmark. Among others, it specifically stipulates regulations concerning the execution of some of the special investigative measures, such as the interception of communications. Article 5.4.2. DCCP assigns the public prosecutor as the central authority to acknowledge and execute an EIO, which in practice is a prosecutor associated with one of the International Legal Assistance Centres (IRC's). In contrast to a regular request for legal assistance, the Ministry of Justice and Security is no longer involved in the judgement and execution of MLA-requests based on the EIO Directive. The IRC's are spread out over several units of the Public Prosecutors Office and are governed by the National Legal Assistance Centre (LIRC). If an EIO is received by any other authority than the IRC, such as an investigative officer or an investigative judge, the EIO will first have to be sent to one of the IRC's in order to acknowledge and execute the requests therein.[370]

---

[369] Article 5.1.12. para. 2 subs a and b DCCP.

[370] Verrest, *T&C Strafvordering*, article 5.4.2. DCCP, comment 2.

Within a week of receiving a request, the issuing State will be notified by the (IRC-) prosecutor of said receipt.

An EIO must meet several requirements before the request can be executed. To formally acknowledge an EIO, article 5.4.3. DCCP contains several standards which have to be fulfilled. First, the request 1) must either be in the Dutch or English language, 2) it must be sent by a competent foreign authority and 3) it needs to contain specific information based on which the formal and substantial requirements for the execution of the request can be tested, especially with regard to the proportionality of the request and possible grounds for refusal. Although the Directive regarding the EIO does not contain any grounds for refusal regarding the proportionality of the request (and even states that a test of proportionality and its interest for the investigation is not possible, as these are to be examined by the issuing State), the Dutch legal framework does have such a provision in article 5.4.3. paragraph 5 DCCP, which provides some form of proportionality testing. The test is, however, only of a marginal nature: when the receiving prosecutor has *serious* doubts regarding the necessity and proportionality of the requested measures in light of the underlying investigation – also considering the rights of the suspect – he can bring these doubts to the attention of the issuing authority. This is also the case if the prosecutor doubts whether the requested measure, under the given circumstances, would be executable in the issuing State.[371] Verrest assumes that these obstacles can easily be circumvented in practice, as the prosecutor will likely be able to request further substantiation of the EIO in order to remove any doubt, or be able to use a less intrusive investigative measure to attain the requested results.[372] The prosecutor is also to confer with his foreign colleagues if he fears that other grounds for refusal apply, thereby providing them the option to further substantiate a request and show that these grounds do not apply. Further grounds for refusal, as well as the aforementioned duty, are given in article 5.4.4. DCCP. In light of the execution of investigative measures, the further grounds are that the request:

1. would breach any principles of privilege, such as the privilege of non-disclosure, the freedom of the press, the freedom of speech or any immunity,
2. would affect the interests of national security by its execution, would compromise the source of information or would entail the surrendering of information of intelligence services that is marked as classified,
3. is issued regarding an investigation into an act that was not committed within the territory of the issuing state but (partially) within Dutch territory, whereby the act is not a criminal act in the Netherlands,
4. might breach fundamental rights if executed (although reasonable grounds for believing such are necessary).

---

371 Article 5.4.3. para. 5 DCCP.

372 Verrest, *T&C Strafvordering,* article 5.4.3. DCCP, comment 3(a).

Two further grounds for refusal are given in article 5.4.4. paragraph 2 DCCP:

1. the execution of an EIO is refused if the act for which the EIO is sent is not punishable according to Dutch criminal law, unless the act is encompassed in Appendix D to the Directive and has a maximum penalty of at least 3 years imprisonment in the issuing Member State (this ground for refusal is an implementation of the principle of dual criminality);
2. the request entails the deployment of an investigative measure for which Dutch criminal procedure demands a higher punitive threshold regarding the criminal act that is investigated: e.g., an interception measure can only be deployed in the Netherlands if a criminal act is investigated for which pre-trial detention can be ordered. If the suspicion does not allow pre-trial detention, the execution of the EIO can be refused.[373]

As has already been mentioned, the proportionality of the requested measure and whether its deployment is necessary for the investigation, is not to be tested by the receiving prosecutor. However, the prosecutor is (if possible) to apply investigative measures other than those requested in the EIO if those measures cannot be used in a Dutch investigation (either because the use of the measure is not possible according to Dutch criminal procedure, or not under the given circumstances),[374] or if the use of another measure would generate the same results while constituting a lesser infringement for those involved.[375]

For the deployment of interception measures, article 5.4.17. DCCP provides additional regulations and constitutes the implementation of the stipulations given in article 30 of the EIO Directive. In addition to the grounds for refusal given in article 5.4.4. DCCP, the deployment of an interception measure can be refused if said deployment would not be granted in a similar national investigation, *including* when the measure would be reviewed as not proportionate. The decision whether the deployment of the measure is *in the interest of the investigation* is to be judged by the foreign authorities, not the receiving prosecutor.[376]

Although the text above shows that the acknowledgement and execution of EIO's is subject to 1) a marginal proportionality test, 2) the possibility to execute other measures that are less intrusive and 3) a set of grounds for refusal, the assessment of EIO's is done in line with the principle of mutual trust, which in practice means that the investigative actions are generally fully performed as requested by the issuing Member State.

---

373 Verrest, *T&C Strafvordering*, article 5.4.4. DCCP, s. 4(b).

374 Article 5.4.7. para. 2 DCCP.

375 Article 5.4.7. para. 4 DCCP.

376 Verrest, *T&C Strafvordering*, article 5.4.17. DCCP, comment 3.

2. Procedure

If the prosecutor is of the opinion that the request for the use of an interception measure can be granted, the execution can either be performed by transferring the communications data in real-time, *or* by intercepting, recording and subsequently transferring the data.[377] A third option, which can be requested by the issuing authority, is that the recording is transcribed, decoded or decrypted by the Dutch authorities, in which case the costs of these proceedings will be passed on to the issuing State.[378] If the issuing authorities are capable of intercepting the communications themselves – therefore without technical assistance of the Dutch authorities – a notification can be sent to the Netherlands, similarly to the notifying possibility provided in article 5.1.13. DCCP under the regular MLA framework.[379] The assessment of the practicability of the request is performed in the same way as when an incoming EIO requests the Dutch authorities to execute an interception measure.[380] When authorization is given based on the notification, the prosecutor attaches to this authorization – while stating the reasons – the conditions imposed by the examining magistrate as well as two conditions. The data obtained by tapping the communications of the user during his stay on Dutch territory:

1. is not to be used and is to be destroyed if it concerns statements by or to a person entitled to the privilege of non-disclosure,
2. may only be used for the investigation for which the authorization is given, unless specific prior authorization is given for the use of the data otherwise.

3. Effect of implementation of the EIO on international cooperation

This examination of the procedure on executing an EIO, as given in the national framework that was implemented in the adaptation of the Directive, shows that no significant changes are to be expected in the cooperation between European nations – especially not in providing legal assistance regarding the interception of communications. The fact that judicial authorities are now able to interchange requests without the intervention of the Ministry of Justice will probably result in even smoother cooperation (at least from a Dutch perspective). The fact that the proportionality of intercepting communications can be tested upon receiving an EIO (whereas this is not allowed in the execution of similar requests following the regular framework on legal assistance) is not expected to have any impact of significance; in addition to the fact that acknowledgement and execution of EIO's is done based on mutual trust and therefore generally executed as requested, interception

---

377 Article 5.4.17. para. 2 DCCP.

378 Article 5.4.17. para. 3 DCCP.

379 See section V.B.1.b.

380 Verrest, *T&C Strafvordering*, article 5.4.18. DCCP, comment 2.

measures are quite frequently used in Dutch investigations and are usually deemed proportionate – EIO's are not likely to be denied because of a lack of proportionality.

In my opinion, the conclusion can be drawn that the introduction of the EIO in national legislation will – from a Dutch perspective – lead to a more effective cooperation, albeit a small increase with regard to the provision on real-time transfer of communications data; the former (regular) framework already provided an adequate basis for such cooperation. However, the implementation of the EIO Directive comes with the introduction of strict time limits in which receiving EIO's must be confirmed and the execution of EIO's must be performed. The real benefits of the introduction of the EIO are therefore to be expected from these time limits.

D. Statistics

Although the statistics on mutual legal assistance are not published as comprehensively as was the case with statistics on national interception in Part A, some figures could be retrieved. In 2013, about 30,000 MLA requests regarding cooperation in investigating, prosecuting, trial and execution of criminal offences were received by the Netherlands. Almost 95% of these requests came from EU Member States, with a majority from Belgium and Germany.[381] In 2016, the total number of incoming requests stayed largely the same and totalled 29,549, whereas outgoing requests totalled 5,964.[382] For both incoming and outgoing requests the majority were again in relation to the neighbouring countries of Belgium and Germany.[383] Regarding assistance in intercepting communications, it has been stated by the National Police and the Public Prosecutors Office that in 2014 a total of 150 requests were received regarding technical assistance in intercepting communications, and a total of 238 requests regarding the real-time transfer of communications data (therefore, without technical assistance). In 2015, these numbers were 147 and 453, respectively.[384]

---

381 Explanatory Memorandum to the Revision, p. 2 (see Appendix).

382 Annual Report of the Public Prosecutor's Office 2016, p. 51.

383 *Ibid*.

384 Impact Analysis, p. 10.

Appendix

Bibliography

1. Literature

Annual Report of the Public Prosecutor's Office 2016

Jaarbericht 2016, Openbaar Ministerie, which can be found at: https://www.om.nl/@98932/jaarbericht-2016/

BIRS 2004

De EU-rechtshulpovereenkomst toegelicht, Bureau Internationale Rechtshulp toegelicht, July 2004.

Corstens/Borgers 2011

G.J.M. Corstens, *Het Nederlands strafprocesrecht*, G.J.M. Corstens & J. Borgers (red), 7th ed., Deventer: Wolters Kluwer 2011.

Corstens/Borgers & Kooijmans 2018

G.J.M. Corstens, *Het Nederlands strafprocesrecht*, J. Borgers & T. Kooijmans (red), 9th ed., Deventer: Wolters Kluwer 2018.

Handboek Strafzaken

M.F. Attinger e.a./P.A.M. Mevis e.a., *Handboek Strafzaken*, Deventer: Wolters Kluwer (online).

Koops 2005

B.J. Koops e.a., *Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet,* Tilburg: TILT 2005.

Koops 2012a

B.J. Koops e.a., *Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing*, Tilburg/Den Haag: TILT/WODC 2012.

Koops 2012b

B.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel - Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelingsplicht voor verdachten?*, Den Haag: Boom Lemma (WODC) 2012.

Koops 2014

B.J. Koops, 'Cybercriminaliteit,' in: S. van der Hof, A.R. Lodder, & G.J. Zwenne (eds), *Recht en Computer*, 6th ed., Deventer: Kluwer 2014, pp. 213–241.

Koops 2016

B.J. Koops, *Criminal investigation and privacy in Dutch law*, Tilburg: TILT 2016 (v1.0), available at http://ssrn.com/abstract=2837483

Koops & Buruma 2007

B.J. Koops & Y. Buruma (2007), 'Formeel strafrecht en ICT,' in: B.J. Koops (red), *Strafrecht en ICT*, 2nd ed., Den Haag: SDU 2007, pp. 77–121.

Koops Committee Report 2018

B.J. Koops e.a., Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, 2018. An English summary of the Koops Committee Report will become available in the course of 2019.

Koops, Conings & Verbruggen 2016

B.J. Koops, C. Conings, & F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht: Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden? (Preadviezen voor de Nederlands-Vlaamse Vereniging voor Strafrecht)*, Oisterwijk: Wolf Legal Publishers (WLP) 2016.

Koops & Oerlemans 2019

B.J. Koops & J.J. Oerlemans, *Strafrecht & ICT*, 3rd ed., Den Haag: SDU 2019.

Kuiper 2014

R. Kuiper, *Vormfouten (Staat en Recht nr. 19)*, Deventer: Kluwer 2014.

Luchtman 2013

M.J.J.P. Luchtman (2013), in: Melai/Groenhuijsen e.a., *Het wetboek van strafvordering*, Deventer: Kluwer (online).

Maessen 2015

H.L.C. Maessen (2015), in: M.F. Attinger e.a./P.A.M. Mevis e.a., *Handboek Strafzaken*, Deventer: Wolters Kluwer (online).

Reijntjes 2017

J.M. Reijntjes, *Minkenhof's Nederlandse strafvordering*, Deventer: Wolters Kluwer 2017.

Stratix 2009

Stratix, *Grenzen aan de aftapbaarheid?*, Hilversum: Stratix Consulting 2009.

T&C Grondwet & Statuut

P.P.T. Bovend'Eert (red.), *Tekst & Commentaar Grondwet & Statuut*, Deventer: Kluwer (online).

T&C Internationaal strafrecht

P.A.M. Verrest (ed), *T&C Internationaal strafrecht*, 7th ed., Deventer: Kluwer (online).

T&C Privacy- en telecommunicatierecht

G.J. Zwenne & P.C. Knol (eds), *T&C Privacy- & telecommunicatierecht,* 6th ed., Deventer: Wolters Kluwer 2018.

T&C Strafvordering

C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen (eds), *Tekst & Commentaar Strafvordering*, 12th ed., Deventer: Wolters Kluwer 2017.

Ter Haar & Van den Brink 2018

R. ter Haar & S.E. van den Brink, *in*: R. ter Haar, G.H. Meijer & A. Seuters/S.E. van den Brink & R. ter Haar, *Leerstukken Strafrecht*, Deventer: Wolters Kluwer 2018.

Van Dartel & Hoekendijk 2016

R.T.J. van Dartel & M.G.M. Hoekendijk, *Zakboek Proces-verbaal en bewijsrecht*, Deventer: Wolters Kluwer 2016.

Van Dijk & Keltjens 1995

Chr.H. van Dijk & J.M.J. Keltjens, *Computercriminaliteit*, Zwolle: Tjeenk Willink 1995.

WODC 2004

A. Beijer e.a. *De Wet bijzondere opsporingsbevoegdheden – eindevaluatie*, Den Haag: WODC 2004.

WODC 2012

G. Odinot e.a., *Het gebruik van de telefoon- en internettap in de opsporing*, Den Haag: WODC 2012.

WODC 2013a

J. Smits e.a., *Glass privacy – An analysis of the problems in implementing the Dutch Police Data Act*, Deventer/Groningen: WODC 2013, to be found at https://www.wodc.nl/binaries/2236-summary_tcm28-72632.pdf

WODC 2013b

I. Helsloot e.a., *An evaluation of the Netherlands Judicial Data and Criminal Records Act (Wet justitiële en strafvorderlijke gegevens, Wjsg)*, Nijmegen: WODC 2013, to be found at https://www.wodc.nl/binaries/2102_summary_tcm28-72075.pdf

2. Articles

Bood 2018

A. Bood, 'Geef ze een vinger… Gedwongen ontgrendeling van een smartphone en het nemo tenetur-beginsel,' *NJB* 2018/1880.

Buruma 2008

Y. Buruma, 'Onprofessioneel politieoptreden,' *DD* 2008/8.

Custers 2018

B. Custers, 'Nieuwe online opsporingsbevoegdheden en het recht op privacy. Een analyse van de Wet Computercriminaliteit III,' *JV* 2018/5.

Kroon-Van Zweeden 2015

M. Kroon-Van Zweeden, 'Het afluisteren van advocaten door de AIVD,' *NJB* 2015/860.

Lintz & Verloop 2009

J.M. Lintz & P.C. Verloop, 'Het professioneel verschoningsrecht: soms zijn er grotere belangen dan de waarheidsvinding in strafzaken,' *DD* 2009/74.

Muijen 2016

P.J.D.J. Muijen, 'Wet computercriminaliteit III. To boldly go where no man has gone before,' *P&I* 2016, p. 104-110.

NJB 2018

'Stb. 2017, 489 Versterking bestrijding georganiseerde criminaliteit,' *NJB*, 10 January 2018 (online).

Oerlemans 2011

J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid,' *DD* 2011/62.

Oerlemans 2012

J.J. Oerlemans, 'De mogelijkheden en beperkingen van de internettap,' *JV* 2012/38.

Oerlemans 2017

J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op internet,' *Strafblad* 2017/4.

Stein & Rossieau 2003

T.H.W. Stein & E.E. Rossieau, 'Digitale opsporingspraktijk in Nederland,' *Computerrecht* 2003/2.

Van Buiten 2016

N. van Buiten, 'De modernisering van de Wet BOB – Herinneren we ons de IRT-affaire nog?,' *DD* 2016/10.

Van der Laan & Newitt 2014

N. van der Laan & B.W. Newitt, 'Tap secret? De strijd tussen transparantie en geheimhouding,' *Computerrecht* 2014/151.

3. Case law

a) International

ECtHR, *P.V. v. Germany,* 13 July 1987, no. 11853/85

ECtHR, *Goodwin v United Kingdom*, 11 July 2002, no. 28957/95

ECtHR, *M.M. v. The Netherlands*, 8 April 2003, no. 39339/98, *NbSr* 2003/185

ECtHR, *Van Vondel v. The Netherlands*, 25 October 2007, no. 38258/03, *NJ* 2008/584, m.nt. Dommering

ECtHR, *Stojkovic v. Belgium & France*, 27 October 2011, no. 25303/08, *NJ* 2013/1, m.nt. Reijntjes

EU CoJ, *Digital Rights Ireland* & *Seitlinger,* 8 April 2014, C-293/12 & C-594/12

b) Supreme Court

HR 10 January 1984, ECLI:NL:PHR:1984:AC1211, m.nt. Th.W. van Veen

HR 29 September 1987, ECLI:NL:PHR:1987:AC9986, NJ 1988/302, m.nt. Th.W. van Veen

HR 19 December 1995, ECLI:NL:HR:1995:ZD0328, NJ 1996/249, m.nt. T.M. Schalken (Zwolsman)

HR 7 May 1996, ECLI:NL:PHR:1996:AB9820, NJ 1996/687 m.nt. Schalken (Dev Sol)

HR 19 March 2002, ECLI:NL:HR:2002:ZD2927, NJ 2002/580

HR 05 September 2006, ECLI:NL:HR:2006:AV4122, NJ 2007/336, m.nt. T.M. Schalken

HR 12 September 2006, ECLI:NL:HR:2006:AV6188, LJN AV6188

HR 13 January 2009, ECLI:NL:HR:2009:BF0837

HR 26 May 2009, ECLI:NL:PHR:2009:BH8800, NJ 2009/261

HR 5 October 2010, ECLI:NL:HR:2010:BL5629, NJ 2011/169

HR 22 May 2012, ECLI:NL:HR:2012:BV9212, *NJ* 2012/399, m.nt. A.H. Klip

HR 5 November 2013, ECLI:NL:HR:2013:1109

HR 10 December 2013, ECLI:NL:HR:2013:1740, NJ 2014/93, m.nt. F. Vellinga-Schoostra

HR 1 July 2014, ECLI:NL:HR:2014:1562

HR 31 January 2016, ECLI:NL:PHR:2006:AU3446, NJ 2006, 365, m.nt. Reijntjes

c) Lower Courts

RvS 20 December 2017, ECLI:NL:RVS:2017:3508

Hof Amsterdam 27 January 2015, ECLI:NL:GHAMS:2015:152, *NJFS* 2015/89

Hof Amsterdam 25 March 2014, ECLI:NL:GHAMS:2014:915 *(Piranha)*

CBb 3 December 2014, ECLI:NL:CBB:2014:438

Rb. Amsterdam 20 December 2007, ECLI:NL:RBAMS:2007:BC0685

Rb. Rotterdam 8 oktober 2008, ECLI:NL:RBROT:2008:BF7620, *NJFS* 2008, 23

Rb. Rotterdam 27 maart 2009, ECLI:NL:RBROT:2009:BH9324

Rb. Zutphen 7 October 2009, ECLI:NL:RBZUT:2009:BJ9577

Rb. Noord-Holland 20 March 2013, ECLI:NL:RBNHO:2013:BZ4987

Rb. Den Haag 11 March 2015, ECLI:NL:RBDHA:2015:2498

Rb. Noord-Holland 29 November 2016, ECLI:NL:RBNHO:2016:9792

Rb. Noord-Holland 14 December 2018, ECLI:NL:RBNHO:2018:11578

4. Legislation

a) International legislation

Convention on Cybercrime

Convention on cybercrime, Budapest, 23 November 2001, E.T.S. nr. 185

EU MLA Convention

Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union

European Convention on Human Rights (ECHR)

Convention for the Protection of Human Rights and Fundamental Freedoms

General Data Protection Regulation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

b) National legislation

aa) Codes & Acts

Computer Crimes Act III

Wet van 27 juni 2018 tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), *Stb*. 2018, 322

Explanatory Memorandum to the Computer Crimes Act III

Kamerstukken II 2015/16, 34 372, nr. 3

Data Production Order Act

Wet van 16 juli 2005 tot wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens), *Stb.* 2005, 390

Dutch Constitution (DC)

Grondwet voor het Koninkrijk der Nederlanden, *Stb*. 1815, 45

Dutch Code of Criminal Procedure (DCCP)

Wetboek van Strafvordering, *Stb*. 1925, 343

Dutch Criminal Code (DCC)

Wetboek van Strafrecht, *Stb*. 1881, 35

Intelligence & Security Services Act (ISSA)

Wet van 26 juli 2017, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2017), *Stb.* 2017, 317

Explanatory Memorandum of the ISSA

Kamerstukken II 2016/17, 34 588, nr. 3

Judicial Data and Criminal Records Act

Wet van 7 november 2002 tot wijziging van de regels betreffende de verwerking van justitiële gegevens en het stellen van regels met betrekking tot de verwerking van persoonsgegevens in persoonsdossiers (Wet justitiële gegevens)

Police Act

Wet van 12 juli 2012 tot vaststelling van een nieuwe Politiewet, *Stb.* 2012, 315

Police Data Act

Wet van 17 oktober 2018 tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, *Stb*. 2018, 401

Source Protection Act

Wet van 4 juli 2018 tot wijziging van het Wetboek van Strafvordering tot vastlegging van het recht op bronbescherming bij vrije nieuwsgaring (bronbescherming in strafzaken), *Stb.* 2018, 264

Special Investigative Measures Act (SIMA)

Wet van 27 mei 1999 tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), *Kamerstukken II* 1996/97, 25 403, *Stb.* 1999, 245

Explanatory Memorandum to the SIMA

Kamerstukken II 1996/97, 25 403, nr. 3, *Stb.* 1999, 245

Telecommunications Act

Telecommunicatiewet, *Kamerstukken II* 1996/97, 25 533, *Stb*. 1998, 610

bb) Decrees

Decree on securing data on telecommunications 2009

Besluit beveiliging gegevens telecommunicatie, *Stb.* 2009, 360

Decree on securing data on telecommunications 2018

Besluit beveiliging gegevens telecommunicatie, *Stb*. 2018, 117

Decree on Telecommunications Data Security (DTDS)

Besluit beveiliging gegevens telecommunicatie, *Stb*. 2009, 350

Decree on telecommunications provision 2000

Besluit verstrekking gegevens telecommunicatie, *Stb.* 2000, 71

Decree on telecommunications provision 2006

Besluit verstrekking gegevens telecommunicatie, *Stb*. 2006, 524

cc) Designations

Designation concerning the use of investigative and coercive measures against lawyers

Aanwijzing toepassing opsporingsbevoegdheden en dwangmiddelen tegen advocaten, *Stcrt*. 2011, 4981

Designation on investigative powers 2011

Aanwijzing opsporingsbevoegdheden, *Stcrt*, 2011, 3240

Designation on investigative powers 2014

Aanwijzing opsporingsbevoegdheden, *Stcrt*. 2014, 24 442

Decree on technical means in criminal procedure

Besluit technische hulpmiddelen strafvordering, *Stb*. 2006, 524

Designation on the use of coercive and investigative measures against journalists

Aanwijzing toepassing dwangmiddelen en opsporingsbevoegdheden bij journalisten, *Stcrt.* 2018, 52664

dd) Regulations

Regulation for the interception of public telecommunications networks and services

Regeling aftappen openbare telecommunicatienetwerken en -diensten, *Stb*. 2016, 535

ee) Other

Amendment Reinforcement of combatting organized crime

Wijziging van het Wetboek van Strafvordering en de Wet op de economische delicten strekkende tot aanpassing van enkele bepalingen betreffende de uitvoering van bijzondere opsporingsbevoegdheden en tot regeling van enkele bijzondere procedures van strafvorderlijke aard en aanverwante onderwerpen met het oog op een doeltreffende uitvoeringspraktijk, *Stb*. 2017, 489

Explanatory Memorandum to the Amendment

Kamerstukken II 2016/17, 34 720, nr. 3

Amendment to the DCCP and any other laws regarding the regulation of international cooperation in criminal matters (revision of the regulation on international cooperation in criminal matters)

Wijziging van het Wetboek van Strafvordering en enkele andere wetten met het oog op het moderniseren van de regeling van internationale samenwerking in strafzaken (herziening regeling internationale samenwerking in strafzaken), *Stb.* 2017, 246

Explanatory Memorandum to the Revision

Kamerstukken II 2015/16, 34 493, nr. 3

Amendment to the Telecommunications Act due to Directive 2002/58/EG

Wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens), *Kamerstukken II* 2007/08, 31 145, nr. 9

Bill to Amend the Telecommunications Act with regard to the retention duty of telecommunications data

Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken (aanpassing bewaarplicht telecommunicatiegegevens), *Kamerstukken II* 2018-19, 34 537

Detailed Statement of Response concerning the Amendment to the Telecommunications Act due to Directive 2002/58/EG

Wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad

van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens), *Kamerstukken II* 2007/08, 31 145, F

Impact Analysis

Impactanalyse betreffende de wijziging van het Wetboek van Strafvordering ter implementatie van de richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (implementatie richtlijn Europees Onderzoeksbevel), see

https://www.rijksoverheid.nl/documenten/rapporten/2017/03/31/tk-bijlage-impactanalyse

Implementation of the European Investigation Order Directive

Wet van 31 mei 2017 tot wijziging van het Wetboek van Strafvordering ter implementatie van de richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (implementatie richtlijn Europees onderzoeksbevel), *Stb.* 2017, 231

Revision of the regulation on international cooperation in criminal matters

Wetsvoorstel tot wijziging van het Wetboek van Strafvordering en enkele andere wetten met het oog op het moderniseren van de regeling van internationale samenwerking in strafzaken (herziening regeling internationale samenwerking in strafzaken), *Stb.* 2017, 246

List of Abbreviations

AIRS	Department of International Legal Aid in Criminal Matters
AIVD	General Intelligence and Security Service
CIOT	Central Information Desk for Research on Telecommunications
DC	Dutch Constitution
DCC	Dutch Criminal Code
DCCP	Dutch Code of Criminal Procedure
DTDS	Decree on Telecommunications Data Security
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EIO	European Investigation Order
EU CoJ	EU Court of Justice
FIOD	Fiscal Information and Investigation Service
I&S	Interception & Sensing, unit of the National Police dedicated to the execution of interception measures for all police agencies
IL&T	Human Environment and Transport Inspectorate
IMSI	International Mobile Subscriber Identity

IMEI	International Mobile Equipment Identity
(L)IRC	(National) Centre for International Legal Assistance
ISS	Intelligence & Security Services, the AIVD & MIVD
ISSA	Intelligence & Security Services Act
ISZW	Inspectorate SZW
MIVD	Military Intelligence & Security Service
MLA	Mutual Legal Assistance
NVWA	Netherlands Food and Consumer Safety Authority
SIMA	Special Investigative Measures Act
TC	Telecommunications Act
VoIP	Voice over IP

Poland*

National Rapporteurs:
Sławomir Steinborn
Stanisław Tosza

* This report outlines the legislation and case law as of March 2019.

Contents

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Security Services with Powers of Telecommunication Interception

1. National security architecture

At the outset it should be explained that Polish law differentiates between two main types of activities which may lead to obtaining evidence, *inter alia*, telecommunication data, for the purposes of the criminal process:

1. operational and exploratory activities *(czynności operacyjno-rozpoznawcze)* – carried out on the basis of police law for the purposes of the prevention and detection of crimes; Polish law does not prohibit performing these activities after the criminal proceedings have been initiated and even more importantly materials obtained as a result of some types of operational and exploratory activities (e.g., operational control) can be used as evidence in criminal proceedings;
2. investigation measures *(czynności procesowe)* – carried out by authorities conducting criminal proceedings and based on the provisions of the Code of Criminal Proceedings; they have a strictly procedural purpose: gathering evidence allowing the determination of whether a crime has been committed and who the perpetrator is, and then to bring case to the court and determine justification of the accusation by the court.

In the Polish system of law enforcement, prevention and prosecution of crime is in primarily the task of the Police. In addition, a number of other authorities have law enforcement competences in their particular domains. It is important to stress that these authorities are also responsible for both prevention and prosecution of offences in their respective fields.

The authority responsible for investigation is the prosecutor who either undertakes it themselves (which is the rule in more serious cases), or it is conducted under their supervision by the Police or within the scope of their competence by other authorities, such as the Border Guard, the Internal Security Agency, authorities of the National Revenue Administration, the Central Anti-Corruption Bureau, the Military Police.

Besides the Police, the following authorities are responsible for preventing crime within the scope of their competences:

– The Internal Security Agency *(Agencja Bezpieczeństwa Wewnętrznego)* – competent for the protection of the internal security of the State and its constitutional order; its tasks include the prevention and detection of offences against the internal security of the State (e.g., espionage, terrorism, corruption, arms trafficking);

– Central Anticorruption Bureau *(Centralne Biuro Antykorupcyjne)* – an authority responsible for combatting corruption in public and economic life and for combatting activities detrimental to the economic interests of the state; its tasks include the prevention and detection of corruption offences and related crimes (e.g., against the judiciary, against the reliability of documents);
– The Border Guard *(Straż Graniczna)* – an authority tasked with protecting the state border, controlling border traffic and preventing and counteracting illegal migration; in this respect, it is competent to prevent and detect offences and prosecute the perpetrators of such offences (e.g., crimes and fiscal offences related to crossing the border);
– Military Counterintelligence Service *(Służba Kontrwywiadu Wojskowego)* – a service competent in matters of protection against internal threats to defence and security of the State as well as the combat capability of the Armed Forces; its tasks include prevention and detection of crimes committed by soldiers on active military service, officers of the Military Counterintelligence Service and the Military Intelligence Service, as well as employees of the armed forces and other organisational units of the Ministry of National Defence, related to the functioning of these services and armed forces;
– Military Gendarmerie *(Żandarmeria Wojskowa)* – tasked with prevention and detection as well as prosecution of offences committed by soldiers and civilian personnel of the army;
– National Revenue Administration *(Krajowa Administracja Skarbowa)* – a government administration dealing with tax, customs and toll revenues; its tasks include, *inter alia*, preventing, detecting, investigating and prosecuting fiscal offences and certain other related offences.

For some authorities, tasks related to prevention and prosecution of crime are linked to their intelligence competence. These are the Internal Security Agency and the Military Counterintelligence Service. Their tasks include collecting and analysing information that may be important for the protection of the internal security of the state and its constitutional order, as well as for its defence. In turn, the Intelligence Agency *(Agencja Wywiadu)* deals, among other issues, with collecting and analysing information important for state security and defence, as well as for the country's international standing.

2. Powers for the interception of telecommunication

a) Law of criminal procedure

Pursuant to provisions of the Code of Criminal Procedure, prosecution authorities are able to intercept telecommunications, as well as gather subscriber and traffic data. This is conditional upon the suspicion, based on specific facts, that a certain offence has been already committed.

b) Preventive law

The interception of telecommunications data is also possible for crime prevention purposes. The Police and some other authorities, whose competences include preventing and combatting crime (Internal Security Agency, Central Anticorruption Bureau, Border Guard, Military Gendarmerie, Military Counterintelligence Service, National Revenue Administration), may, within so-called operational and exploratory activities *(czynności operacyjno-rozpoznawcze)*, carry out operational control *(kontrola operacyjna)*. Operational control has to be conducted confidentially and is the obtaining and recording of the content of conversations conducted via the use of technical means, including by telecommunications networks, obtaining and recording of image or sound of persons on premises, in means of transport or in non-public places; it can also consist of obtaining and recording the content of correspondence, including electronic correspondence, data contained on IT data carriers or on telecommunications terminal equipment, within IT and ICT systems, as well as in obtaining access to and controlling the content of mailed packages. Operational control may be carried out not only with the aim of prevention, investigation and detection of criminal offences, but also in order to identify and prosecute concrete offenders and to obtain and preserve evidence.[1]

Operational control may be ordered in respect of serious offences that are listed in the law. It has to be ordered by the district court[2] at the request of a competent authority submitted after obtaining the prosecutor's consent. Initially it can be ordered for three months, but with a possibility of an extension up to 12 months. It can be ordered and carried out also in the course of an investigation already in process against a concrete person.[3] The crucial importance of operational control in the Polish system is the fact that evidence collected in the course of operational control can be used at trial without any particular limitation.[4]

The Police and other authorities entitled to request and conduct operational control also have the right to request telecommunications data (subscriber and traffic data) from telecommunications service providers.[5] The data is transmitted to these authorities without the knowledge of the persons concerned. In the framework of this measure, data can be also acquired directly via the telecommunications network through the access of an authorised officer to the system of a given operator,

---

[1] See more *D. Szumiło-Kulczycka*, Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego, Warszawa 2012, pp. 173–180.

[2] Judiciary in Poland (competent for criminal cases) consists of county courts *(sądy rejonowe)*, district courts *(sądy okręgowe)*, courts of appeal *(sądy apelacyjne)* and at the highest level – the Supreme Court.

[3] *D. Szumiło-Kulczycka*, Czynności, p. 183.

[4] E.g., Art. 19 (15) Law of 6 April 1990 on Police (Journal of Laws of the Republic of Poland 2019, pos. 161).

[5] E.g., Art. 20c Law on Police.

provided that such access is technically appropriate. This access is done with knowledge and cooperation of the service provider. Regardless of the form of the acquisition of data, no court or prosecutor's order is required. However, in contrast to operational control, the acquisition's purpose is prevention or detection of crime only, as data obtained in this way cannot be used to identify a concrete offender or as evidence in trial.[6]

c) Law of intelligence agencies

Both the Internal Security Agency and the Military Counterintelligence Service may secretly obtain telecommunications data (subscriber and traffic data) in order to achieve their mission.

In the case of a foreigner against whom there is suspicion that they may be carrying out terrorist activities, the Head of the Internal Security Agency may order the interception of the content of calls made over telecommunications networks as well as of the correspondence made using electronic means of communication, as well as data contained in telecommunications systems. Curiously, *a contrario*, such a measure cannot be applied to a Polish citizen.[7]

3. Responsibility for the technical implementation of interception measures

The technical implementation of interception measures is done by state agencies authorised to gather telecommunications data in this way. The telecommunications service providers are obliged to provide primarily technical assistance during the implementation of these measures. There is no one centralised institution competent for the technical implementation of interception of telecommunications, but rather each competent authority implements interception itself.

4. Legitimacy of data transfers between security agencies

There is no direct regulation on transfer of telecommunications data gathered under different regimes from one competent authority to another. Provisions of the CCP do not provide for any restrictions on the use of data obtained during criminal proceedings for prevention or intelligence purposes. It therefore seems that the general provisions on access to the case files apply, from which it should be derived that the prosecutor and the court can, in exceptional cases, make these files available to persons other than the parties.

---

[6] *D. Szumiło-Kulczycka*, Czynności, pp. 269–270.

[7] Art. 9 Law of 10 June 2016 on anti-terrorist measures *(ustawa o działaniach antyterrorystycznych)*, Journal of Laws of the Republic of Poland 2018, pos. 452.

In turn, it can be concluded from some regulations of Law on Police that it is admissible to transfer data obtained as a result of operational and exploratory activities between authorities and services authorised to conduct them. According to Art. 20b (1) Law on Police, the Police may provide such authorities with information on operational and exploratory activities as well as on the means used and methods of their accomplishment. Pursuant to Art. 14 (4) Law on Police, in order to fulfil statutory tasks the Police may use data about the person, including electronic records, obtained by other authorities, services and state institutions as a result of performing operational and exploratory activities, and process them without knowledge and consent of the person concerned.

The provisions regulating the functioning of intelligence agencies (Intelligence Agency, Military Intelligence Service) also lead to the conclusion that these agencies are entitled to obtain personal data and other information gathered by other agencies and services as a result of operational and exploratory activities.[8]

B. Statistics on Telecommunication Interception

Since 2016 district courts have been obliged to compile statistics on processing telecommunications, postal and internet data by the prosecuting agencies (Police and others). These statistics are delivered to the Minister of Justice, who is obliged to present annual information to the Parliament on processing telecommunications, postal and internet data by the prosecuting agencies.

Processing data by the prosecuting agencies			
Year	Telecommunications data	Postal data	Internet data
2016	1,147,092	1,806	23,150
2017	1,227,314	13,360	23,913

In 2016 among telecommunications data obtained by the prosecuting agencies were: 76.9 % – billings, 13.6 % – location data, 7 % – user data, 2.5 % – other.

The Attorney General is also obliged to present to the Parliament explicit annual information on the total number of persons against whom a request has been made to order interception of conversations and other transfers of information (Arts. 237–242 CCP) or to order an operational control.

[8] Art. 34 Law of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (Journal of Laws of the Republic of Poland 2018, pos. 2387); Art. 38 Law of 9 June 2006 on Military Intelligence Service and Military Counterintelligence Service (Journal of Laws of the Republic of Poland 2017, pos. 1978).

Interception of conversations and other transfers of information and operational control				
Year	Total number of requests	Number of accepted requests	Number of refusals by the courts	Number of requests unaccepted by the prosecutors
2011	5,188	4,863	39	286
2012	4,206	3,956	25	225
2013	4,509	4,278	16	215
2014	5,435	5,221	12	202
2015	5,673	5,431	20	222
2016	6,035	5,881	45	109
2017	6,562	6,402	14	146

II. Principles of Telecommunication Interception in Constitutional and Criminal Procedural Law

A. Constitutional Safeguards of Telecommunication

1. Areas of constitutional protection

The analysis of protection of relevant values was undertaken in the fundamental and explicatory judgment of the Polish Constitutional Tribunal of 2014,[9] which set the conceptual framework of the protection of rights and freedoms in the context of collecting data on individuals by technical means in operational (law enforcement) activities. That reflection on the rights and freedoms remains valid and this section is based on the analysis and views expressed by the Tribunal therein.

Personal liberty is the most natural feature of the legal status of an individual.[10] This status is linked with human dignity safeguarded by the Polish Constitution in Art. 30, the first and most crucial right guaranteed by the Constitution. It is the cornerstone of the framework of protection. The guarantee of freedom of the human

[9] Judgment of the Constitutional Tribunal of 30 July 2014, K 23/11, OTK-A 2014, No. 7, pos. 80 (Judgment TK K 23/11). On this judgment, see also *B. Grabowska-Moroz*, Ochrona gromadzonych danych telekomunikacyjnych i zasady ich udostępniania na tle Konstytucji RP i prawa Unii Europejskiej – glosa do wyroku Trybunału Sprawiedliwości z 8.04.2014 r. w sprawach połączonych: C-293/12 i C-594/12 Digital Rights Ireland oraz do wyroku Trybunału Konstytucyjnego z 30.07.2014 r. (K 23/11), Europejski Przegląd Sądowy 2016, No. 1, pp. 31–36.

[10] Judgment TK K 23/11, III 1.2.

being *(wolność człowieka)* is expressed in Art. 31 Constitution and is protected in both its positive and negative aspects. As to the positive aspect, human beings can decide freely what they do or not do. As to the negative aspect, others should refrain from intruding into the sphere which is reserved for the individual and the State should guarantee that.[11] The conditions for legal limitations of human liberty are expressed in Art. 31 (3): "Restrictions on the use of constitutional freedoms and rights may be established only in the law and only if they are necessary in a democratic state for its security or public order, or for the protection of the environment, health and public morals, or the rights and freedoms of others. These limitations shall not violate the essence of freedoms and rights." These limitations should pass the test of proportionality.[12]

In order to guarantee human dignity and liberty the Constitution protects the right to private life (Art. 47). This is not considered to be a right that is given to the human being by the Constitution, but as a (natural) liberty which the Constitution protects.[13] The limitations to this right may only be provided for by a statute.

Furthermore, Art. 51 protects "information autonomy."[14] This article stipulates in particular that "no one shall be obliged, other than in a statute, to disclose information concerning him or her." It requires that public authorities collect data on individuals only to the extent that it is indispensable in a democratic state upholding the rule of law, and guarantees the right of an individual to information about the data collected by the authorities and the right to have it corrected or deleted, in particular if it was collected illegally.

Arts. 47 and 51 protect the same sphere – privacy.[15] A string of judgments of the Constitutional Tribunal confirms that information autonomy is the crucial element of the right to private life and consists of the autonomous decision on disclosing to others information about oneself and maintaining control over this information even when the information is already in the possession of other persons.[16]

These two provisions are also linked with the right to protection of secrecy of communication guaranteed by Art. 49 Constitution. It stipulates that: "Freedom and protection of confidentiality of communication shall be ensured. Their limitation may take place only in the cases specified in a statute and in the manner specified therein." Communication for this article's sake should be understood as direct

---

[11] Judgment TK K 23/11, III 1.2.

[12] Judgment of the Constitutional Tribunal of 18 February 2004 r., P 21/02, III 4.

[13] Judgment TK K 23/11, III 1.2.

[14] Judgment TK K 23/11, III 1.3.

[15] *M. Wild,* in: M. Safjan, L. Bosek (eds.), Konstytucja RP. Komentarz, vol. I (Arts. 1–86), Warszawa 2016, p. 1222, marginal no. 3.

[16] Judgment of the Constitutional Tribunal of 13 December 2011, K 33/08, OTK-A 2011, No. 10, pos. 116, III 6.1.

communication between persons and communication by means allowing for long distance exchanges.[17]

The three articles protect all forms of communication, regardless of the distance, types of tools used, etc. They cover all aspects of the exchange, not only its content, but also metadata, location data, information about the IP-number or Internet websites accessed.[18] The constitutional guarantee of freedom of the human being and information autonomy cover also protection against secret surveillance and wire-tapping including communication made in public places. This protection covers private and professional aspects of one's life.

The Tribunal underlined that the communication tools stemming from the development of information and communication technologies are protected by the same guarantees as described above, even if they were written before the digital revolution swept through Poland (the Constitution dates from 1997).[19] This of course does not prevent the legislator from addressing issues such as use of digital technologies to commit or facilitate crime. On the contrary, it is the duty of the legislator to do so in view of the state's duty to guarantee citizens' safety (Art. 5 Constitution) and also in order to fulfil Poland's international obligations. Yet, the legislator, while allowing law enforcement to use new technologies in order to secretly acquire data and evidence, should respect the above rights and freedoms and take into account the specificities of these technologies.[20]

In order to complete the picture, one should also mention Art. 50 Constitution that safeguards the inviolability of the home, which could also be affected by investigation measures. Searches of homes may only be conducted upon powers granted in and according to conditions described by a statute. This right was not subject to a detailed analysis by the Tribunal. Nevertheless, investigation undertaken by law enforcement may potentially violate this right, particularly given the expectation of privacy. It has been suggested in the literature, however, that the right to privacy should be focused on the Art. 47 right to private life.[21]

In view of this set of guarantees provided by the Constitution "obtaining information about the private life of individuals by public authorities, in particular secretly, must be limited to necessary situations, admissible in a democratic state and only for the protection of constitutionally recognised values and in accordance with the principle of proportionality. The conditions for the collection and processing of this data by public authorities must be regulated in statutes in the most transparent

---

[17] Judgment of the Constitutional Tribunal of 20 June 2005 r., K 4/04, OTK-A 2005, No. 6, pos. 64.

[18] Judgment TK K 23/11, III 1.4.

[19] Judgment TK K 23/11, III 1.5.

[20] Judgment TK K 23/11, III 1.7.

[21] *M. Wild*, in: M. Safjan, L. Bosek (eds.), Konstytucja, p. 1212, marginal nos. 24–25.

manner, excluding arbitrariness and arbitrariness of their application."[22] It is thus certainly not permitted to record the entirety of an individual's private life.[23]

In conclusion, the measures that consist of some form of investigation through digital means must pass the test on proportionality (Art. 31 (3)) and be prescribed in a statute in a sufficiently precise way. The latter condition stems in particular from Art. 2 Constitution, which declares that Poland upholds the rule of law.

2. Proportionality of access to data

As mentioned above, the principle of proportionality is declared in Art. 31 (3) Constitution and is crucial in the assessment of infringement of the right described in the previous section (see above). Proportionality considerations were used by the Supreme Court when assessing the use of information obtained through operational control in relation to other offences or other persons as to which/whom the operation control was initially ordered. These considerations did not stop the Court from allowing such use.[24] Furthermore, regular courts are obliged by the Constitution to apply a proportionality test even where the CCP does not contain this obligation. For that reason, as we explain below, the court shall consider, *inter alia*, whether other means of investigation less intrusive than electronic communication interception are likely to be successful. However, since the requirement is not in the CCP, in practice consideration is not often given to the principle of proportionality.[25]

Moreover, boundaries given by the Constitution can play an important role when the law does not offer protection. For example, criminal procedural law does not provide specific safeguards excluding communication in a "core area of private life" from interception. However, the question of the admissibility of the interception of such content as prayers, communication during sexual activities, diaries, etc. may be taken into consideration through the constitutional principle of proportionality.

As to access to traffic and location data, the Constitutional Tribunal in the judgment mentioned above stressed the need to respect the principle of proportionality when designing the rules on gathering this category of data. The Tribunal pointed out (citing the *Digital Rights Ireland* judgment[26]) that sufficient amount of this kind of data, when properly analysed, may give an extensive profile of the person's life. The knowledge that the authorities gather this kind of data, often in a way which does not allow the persons concerned to notice that fact, may give the im-

---

22 Judgment TK K 23/11, III 1.12.

23 Judgment TK K 23/11, III 1.14.

24 See more in details under IV.3.a.

25 See also below III.B.7.

26 CJEU, 8 April 2014, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland.

pression of being constantly watched and this infringes fundamental rights. However, the possibility of gathering this kind of data may be extremely helpful in fighting crime, hence the need for a proper analysis of proportionality of gathering of traffic and location data.[27]

3. Consequences for the interception of telecommunication

The constitutional standard of protection of secrecy of communication was analysed in the above-mentioned judgment of the Constitutional Tribunal of 2014. The Tribunal established a set of conditions that a legal framework must comply with when infringing the constitutional rights analysed in part 1 of this section. In general the provisions must be precise and proportionate. How it translated into more precise conditions will now be described.

As to the requirement of precision of the legal framework, limitations of the right to private life (stemming from law enforcement secret investigation) should be established in a statute,[28] which precisely states the conditions for applying the prescribed measures, with vague references to protected legal interests not being sufficient. The catalogue of offences to which the measures should be applicable should also be precise and limited to what is necessary.[29] This statute must also precisely describe the way in which the law enforcement is allowed to infringe the right, and to which categories of persons it may be applied.[30] The former does not mean that the law must contain a very precise technical description of the measures. That would risk rendering them quickly technically obsolete and unnecessary casuistic.[31] It is also necessary that the period for which the measure may be applied be limited and precisely defined.[32] The statute must also precisely prescribe the competence and the procedure for ordering such measures, using and destroying their outcome. Ordering the measure and the review of its legality should be done by an authority independent from the executive branch of the government, preferably by a court.[33]

In terms of being proportionate, the measure must be aimed at defending the democratic values of a rule of law state, values that have their basis in the Constitution. Detection and prosecution of serious crime can be such an aim. Yet, these measures should be the least onerous for achieving these aims, and applied only

---

[27] Judgment TK K 23/11, III 1.11.

[28] Judgment of the Constitutional Tribunal of 12 December 2005 r., K 32/04, OTK-A 2005, No. 11, pos. 132.

[29] Judgment TK K 23/11, III 5.1.3.1.

[30] Judgment TK K 23/11, III 5.3.

[31] Judgment TK K 23/11, III 5.1.3.2.

[32] Judgment TK K 23/11, III 5.1.3.3.

[33] Judgment TK K 23/11, III 5.1.3.4-5.1.3.5.

exceptionally, and only when they can bring meaningful results.[34] The subsidiarity of the use of these measures is linked to the necessity of independent (from the law enforcement) control and review of the application of such measures that should be ideally executed by the courts.[35] In order for the control to be meaningful, the independent authority should have sufficient competences and provide reasons for its decisions. While control *ex ante* should be the rule, *ex post* review is allowed as an exception.[36]

To this, further procedural guarantees should be added, notably the duty to inform the person concerned about the measure, although this can be done after the performance of the measure in order to guarantee that its aim can be achieved. The authorities should make public statistical information on the use of investigation measures.[37] They must also guarantee the security of the data from attacks by third parties.[38]

There is no protection of the confidentiality and integrity of information systems at the constitutional level, besides the aspects that were discussed above. The Criminal Code (CC) contains a number of offences protecting confidentiality of information and integrity of information systems in the chapter on offences against the protection of information (Arts. 265–269c). In particular Art. 269a CC punishes a person who, without being authorised to do so, by transmission, destruction, deletion, damage, hindering access to or alteration of IT data, significantly interferes with the operation of an IT system, an ICT system or an ICT network.

There is no specific protection of the core area of privacy. In theory the intercepted communication concerning highly private aspects of life such as sexual activities or prayers may be considered evidence, unless it infringes the principle of proportionality.

4. Statutory protection of personal data

Besides the legal framework of the protection of personal data,[39] the Criminal Code contains two offences aimed at protecting secrecy of information: one regarding the illicit use of information and one regarding access to it.

---

[34] Judgment TK K 23/11, III 5.2.1-5.2.3. Also, for instance, Judgment of the Constitutional Tribunal of 12 December 2005 r., K 32/04.

[35] Judgment TK K 23/11, III.

[36] Judgment TK K 23/11, III 5.2.5.

[37] Judgment TK K 23/11, III 5.2.6.

[38] Judgment TK K 23/11, III 5.3.

[39] Besides the EU instruments, the Law of 10 May 2018 on the protection of personal data *(Ustawa o ochronie danych osobowych)*, Journal of Laws of the Republic of Poland 2018, pos. 1000, 1669 and the Law of 14 December 2018 on the protection of personal data processed with regard to prevention and combatting of criminality *(Ustawa o ochro-*

Art. 266 CC punishes persons who in contravention of the legal requirements reveal or use information that they acquired while executing their public function. This provision could be used in particular to punish public officials (members of authorities entitled to gather data) who reveal information acquired in the process of executing their duties.

Another provision punishes a person who without permission obtains access to information not intended for them, connecting to the telecommunications network or breaking or bypassing electronic, magnetic, informatic or other specific safeguards, as well as a person, who in order to obtain information to which they are not entitled, establishes or uses a tapping device, a visual device or other device or software (Art. 267 CC). The same article extends criminal liability also to persons who in order to get information to which they are not entitled, install or use a wiretapping or similar device. It is also punishable to pass information thus acquired to another person. This provision may also be used to punish public officials who access or try to access phones, computers or similar devices in disrespect of legal provisions.[40]

Another aspect of protecting secrecy of communications is constituted by the rules on secrecy for certain professions. They directly affect the possibility of gathering the content of communications made by members of that profession. These provisions concern in particular defence councils and priests and, to a lesser extent, notaries, attorneys, legal advisers, tax advisers, medical doctors and journalists.[41]

The principle of "purpose limitation of personal data" is not absolute in Polish criminal proceedings. The CCP does not forbid the use of data collected by law enforcement during operational control for a different offence or concerning a different person than initially ordered.[42]

B. Powers in the Code of Criminal Procedure

1. Requirement of (reasonable) clarity for powers in the law of criminal procedure

The Code of Criminal Procedure does not contain the requirement of clarity, but it is interpreted from Art. 2 Constitution (rule of law in a democratic state). The Constitutional Tribunal declared this requirement to be one of the crucial rules of law, hence the legislator has the duty to fulfil this desideratum to the maximum

---

nie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości), Journal of Laws of the Republic of Poland 2019, pos. 125.

[40] See also below III.B.11.

[41] For a more detailed analysis see below B.3.

[42] See more in details under IV.3.a.

possible extent, given the particularities of the domain being regulated.[43] 'The provisions on the status of an individual should be "correct," "precise," and "clear."'[44] Yet, if these criteria are not fulfilled, the law does not have to be declared contrary to the Constitution, provided that its imperfection can be repaired by means of legal interpretation.[45] The provisions must be precise enough to understand who is subject to the regulation limiting individual rights and who and under what conditions the measure limiting the rights may be executed.[46] The greater the limitation on individual rights and freedoms by the provision, the greater the necessary precision.[47] However, norms are allowed to, or perhaps even must avoid the casuistic approach, which runs the risk of becoming technologically obsolete in a short time.[48]

Furthermore, a regulation on infringing the secrecy of communication would also be contrary to Art. 31 (3) and Art. 49 Constitution.[49]

2. Differentiation and classification of powers in the law of criminal procedure

The provisions that will be discussed below are contained in two chapters of the Code of Criminal Procedure, in this sense they are specifically described by the law. However, one of the chapters is about search and seizure in general. The second one is also imperfect, as it was written in the times when the traditional phone was common, and the cell phone was rather new, not to mention the Internet and smartphones. It is therefore not well adjusted to modern times.

It should be mentioned that in order to adapt the Code to the needs of this new digital reality, the provisions have been changed several times. This has caused controversies and debates, for instance as to the admissibility of evidence and the use of evidence for prosecuting a person other than the original subject of the measures in question, or the same person, but for offences other than those indicated in the order for the measure (see more in detail below IV.2. and 3.a.).

---

[43] Judgment of the Constitutional Tribunal of 28 October 2009, Kp 3/09, III 6.2, OTK-A 2009, No. 9, pos. 138.

[44] Judgment TK K 23/11, III 5.1.1.

[45] Judgment of the Constitutional Tribunal of 28 October 2009, Kp 3/09, III 6.3.1.

[46] Judgment TK K 23/11, III 5.1.1; judgment of the Constitutional Tribunal of 30 October 2001, K 33/00, OTK 2001, No. 7, pos. 217, III 3.

[47] Judgment TK K 23/11, III 5.1.1.

[48] Judgment TK K 23/11, III 5.1.3.2.

[49] *M. Wild*, in: M. Safjan, L. Bosek (eds.), Konstytucja, p. 1215, marginal no. 19.

III. Powers for Accessing Telecommunication Data in the Law of Criminal Procedure

A. Overview

The interception of ongoing telecommunications during criminal proceedings is regulated in chapter 26 CCP (Arts. 237–242 CCP). Obtaining of communication data saved in IT systems or on storage media is regulated in Art. 236a CCP, which mandates the respective application of the provisions regulating the search and seizure of this type of data (Arts. 219–236 CCP). Access to traffic data is regulated in Arts. 218–219b CCP.

B. Interception of Content Data

1. Statutory provisions[50]

Article 237

§ 1. After the commencement of proceedings, the court, on the request of the prosecutor may order surveillance and recording of the content of telephone conversations, in order to detect and gather evidence for the pending proceedings or to prevent a new offence being committed.

§ 2. In urgent cases, the surveillance and recording of conversations may be ordered by the prosecutor who is, however, obliged to request an approval of the court within 3 days. The court issues the decision within 5 days in a hearing without participation of the parties. In the event of refusal to approve the prosecutor's order, the court orders in decision concerning the prosecutor's request, that all recordings shall be destroyed. An appeal against this decision stays its execution.

§ 3. The surveillance and recording of the content of telephone conversations is allowed only when the pending proceedings or a justified concern that new offence might be committed pertain to:

1) homicide,

2) general endangerment to life and health or causing a disaster,

3) humans trafficking,

4) kidnapping,

5) demanding ransom,

6) hijacking of an aircraft or a ship,

7) robbery, aggravated theft and extortion,

8) attacking the independence and territorial integrity of the State,

9) attacking the constitutional order of the State or on its supreme agencies, or a unit of the Armed Forces of the Republic of Poland,

---

[50] Throughout the text, when referring to provisions of the Code of Criminal Procedure, the authors use the translation made by *J.E. Adamczyk*, Kodeks postępowania karnego. The Code of Criminal Procedure, Warszawa 2018. However, the authors made alterations to this translation, where it seemed to be necessary.

10) espionage or disclosing a secret information classified “confidential” or “strictly confidential,”

11) amassing weapons, explosives or radioactive materials,

12) the forging and circulating counterfeit money, payment bills or instruments, or transferable documents enabling the acquisition of money, goods, a load or a benefit in-kind or imposing an obligation to pay out capital, interest, share in profit or confirming participation in a company,

12a) counterfeiting or falsifying invoices or using counterfeit invoices or invoices indicating false data, which may have impact on the determination of public dues, its reimbursement or reimbursement of other dues of fiscal nature, as well as issuing and using invoices indicating false data, which may have impact on the determination of public dues, its reimbursement or reimbursement of other dues of fiscal nature,

13) manufacturing, processing, trafficking and smuggling drugs, their precursors, substitutes or psychotropic substances,

14) organised criminal group,

15) property of significant value,

16) the use of violence or unlawful threats in connection with criminal proceedings,

16a) giving a false testimony or providing a false opinion or translation by an expert or translator,

16b) falsely accusing another person of an offence, fiscal offence or a fiscal misdemeanour,

16c) creating false evidence or undertaking other deceitful acts directing against another person a prosecution for an offence, fiscal offence or a fiscal misdemeanour,

16d) concealing evidence proving innocence of a person prosecuted for an offence, fiscal offence or a fiscal misdemeanour,

16e) informing a prosecuting authority about an offence, which has not been committed,

16f) assisting in avoiding criminal liability,

16g) not reporting an offence despite the obligation,

17) bribery and racketeering,

18) pimping, procuring and forcing into prostitution,

19) offences defined in Chapter XVI of the Criminal Code and in Articles 5-8 of the Rome Statute of International Criminal Court.

§ 3a. Surveillance and recording of the contents of telephone conversations is also permissible in order to disclose assets subject to forfeiture referred in Article 45 § 2 of the Criminal Code and Article 33 § 2 of the Fiscal Criminal Code.

§ 4. Surveillance and recording of the contents of telephone conversations is permissible with regard to a suspected person, the accused, victim or any other person whom the accused may contact or who might be connected with the offender or with the potential offence.

§ 5. Offices and institutions conducting telecommunications activity, as well as telecommunications enterprises within the meaning of the Act of 16 July 2004 Telecommunications Law, are obliged to facilitate the execution of a court or prosecutor’s order concerning the surveillance of telephone conversations and to ensure the registration of the fact that such surveillance took place.

§ 6. Only the court and prosecutor shall be entitled to play the recordings, and in urgent cases, the Police with the consent of the court or the prosecutor.

§ 7. The register of telephone conversation surveillance may be examined by the court and in the pre-trial proceedings by the prosecutor.

Article 237a

If, as a result of a surveillance evidence was obtained indicating that a person, against whom the surveillance was ordered, has committed an offence prosecuted *ex officio* or a fiscal offence other than the offence, against which the surveillance was directed, or that such an offence or fiscal offence was committed by another person, the prosecutor decides whether this evidence will be used in criminal proceedings.

Article 238

§ 1. The surveillance and recording telephone conversations may be conducted for a period not exceeding 3 months, which may be extended in particularly justified cases for a period not exceeding a further 3 months.

§ 2. The surveillance should be ended immediately after the circumstances mentioned in Article 237 § 1-3 have ceased to exist, yet no later than with the expiry of the period for which it was imposed.

§ 3. The prosecutor, after the surveillance has ended, submits a motion that all recordings be destroyed, if they are in their entity irrelevant to the criminal proceedings. The court decides about the motion immediately, in a hearing without participation of the parties.

§ 4. After the conclusion of pre-trial proceedings, the prosecutor submits a motion to destroy that part of the recordings that is irrelevant to the criminal proceedings during which the surveillance and recording of telephone conversations was ordered, and which does not constitute evidence referred to in Article 237a. The court decides about the motion in a hearing, which the parties may attend.

§ 5. A motion for an order to destroy recordings may also be submitted by the person referred in Article 237 § 4, not sooner than after conclusion of the pre-trial proceedings. The court decides about the motion in a hearing, which the parties and the petitioner may attend.

Article 239

§ 1. Notification of the order imposing the surveillance and recording of telephone conversations to the person concerned may be adjourned for a period necessary to protect the interests of the case.

§ 2. In pre-trial proceedings notification of the order referred to in § 1 may not be adjourned further than until the conclusion of proceedings.

Article 240

An order concerning surveillance and recording of telephone conversations shall be subject to interlocutory appeal. In the appeal the person concerned with the order may request that both grounds and legality of the surveillance and recording of telephone conversations be examined. The appeal against the order issued by the prosecutor is examined by the court.

Article 241
The provisions of this chapter shall apply respectively to surveillance and recording by technical means of the content of other conversations or information transmissions, including correspondence sent by e-mail.

2. Scope of application

a) Object of interception

Interception of communication in Polish criminal proceedings is regulated on two levels. Almost the all provisions in chapter 26 CCP titled "Surveillance and recording of conversations" concern what this chapter defines as the object of interception, namely the "content of telephone conversations" *(treść rozmów telefonicznych)*. In the next step Art. 241 CCP extends the application of these provisions to the content of conversations and transfers of information other than telephone conversations.

"Telephone conversations" refers both to calls by landline and by mobile phones. The reference to "other conversations" in Art. 241 CCP thus should be understand as "other conversations than telephone conversations" and includes conversations conducted without the use of any technological means. The term "other transfers of information" is extremely wide. This provision explicitly indicates one type: correspondence sent by email. Art. 241 CCP extends the application of the provisions regarding the interception to transfers of information such as analogous data communication via landlines (e.g., fax), radio communication, and communication via internet.[51] This last means of communication includes VoIP communication,[52] transfer of files between two users, and communication on social networks. It is not limited to person-to-person-communication. The object of interception may also be IP-traffic between a person and an automated information system (such as communication with a webserver while downloading a website)[53] and IP-traffic between a person's computer and their data storage in a cloud or other remote storage of data processing systems.[54] Traffic with the cloud is seen as the communication between the user and the cloud provider. Transfer of information pursuant to Art. 241 CCP covers also IP-traffic between two independent computer systems. The only restriction is that the interception must be applied to a specific person, and therefore these computer systems must belong to specific people who are subject to interception.

---

[51] *P. Hofmański, E. Sadzik, K. Zgryzek*, Kodeks postępowania karnego. Komentarz, Warszawa 2011, vol. 1, p. 1319; Decision of Supreme Court of 21 March 2000, I KZP 60/99, OSNKW 2000, No. 3–4, pos. 26.

[52] *A. Kiedrowicz*, Zagadnienie kontroli przekazów informacji w ramach telefonii internetowej, Prokuratura i Prawo 2008, No. 10, pp. 129–130.

[53] *P. Kosmaty*, Podsłuch komputerowy. Zarys problematyki, Prokurator 2008, No. 4, p. 37.

[54] See *J. Kudła, A. Staszak*, Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze, Prokuratura i Prawo 2017, No. 7–8, pp. 53–56.

There is controversy in the academic literature as to the admissibility of such forms of surveillance that consist of taking over computer data using the analysis of electromagnetic waves emitted by computer hardware (e.g., computer, wires, computer mouse, monitor) or acoustic waves emitted by printers.[55] Some practitioners consider that in these cases there is no conversation or transfer of information in the meaning of Art. 241 CCP and therefore these forms of surveillance are not covered by Art. 241 CCP.[56]

Provisions of CCP do not differentiate clearly between traffic data and content data. Arts. 237 and 241 CCP refer solely to the content of conversations and other information transmissions. The differentiation between traffic data and content data is contained in the ordinance of the Minister of Justice of 24 June 2003, issued pursuant to Art. 242 CCP.[57] According to § 5 of that ordinance, entities involved in the telecommunications business are obliged to collect various types of data tied to the controlled and recorded transmission of information. Next, that data should be added to the carrier which contains recorded transmissions of information. The above suggests clearly that under this regulation, traffic data is treated differently to content data. At the same time, Art. 49 Constitution stipulates that the secrecy of communication may be limited only in cases and in a manner defined in a statute regulating this sphere, and provisions of chapter 26 CCP completely leave out the issue of real-time interception of traffic data.[58] In view of that, one may question whether the law provides an adequate legal basis for interception of traffic data. This doubt can be rebutted however with the following *a maiore ad minus* argument: since the interception of communication requires meeting high-level requirements, it could be assumed that its collection permits the collection of traffic data linked to it.

b) Temporal limits of telecommunication

Provisions of CCP for content interception cover communication data only during its transmission. Content of information already received by the user and stored in their personal system (e.g., hard drive of computer or mobile phone) cannot be the object of interception under Art. 237 CCP. The same applies to the information (e.g., content of emails) stored in the cloud. For example, emails can be intercepted

---

[55] For: *P. Hofmański, E. Sadzik, K. Zgryzek*, Kodeks, vol. 1, p. 1319; *K. Boratyńska*, Podsłuch komputerowy – zagadnienia wybrane, in: E.W. Pływaczewski (ed.), Aktualne problemy prawa karnego i kryminologii, Białystok 2005, p. 16.

[56] See *P. Kosmaty*, Podsłuch, p. 40.

[57] See the Ordinance of the Minister of Justice of 24 June 2003 (rozporządzenie Ministra Sprawiedliwości z 24.6.2003 r. w sprawie sposobu technicznego przygotowania sieci służących do przekazywania informacji, do kontroli przekazów informacji oraz sposobu dokonywania, rejestracji, przechowywania, odtwarzania i niszczenia zapisów z kontrolowanych przekazów), Journal of Laws of the Republic of Poland 2003, No. 110, pos. 1052 – thereafter referred to as "the Ordinance of 24 June 2003."

[58] See *A. Lach*, Dowody elektroniczne w procesie karnym, Toruń 2004, pp. 75–77.

only at the time of their transmission on the network. Acquiring the content of a message stored on a server or in the cloud from the telecommunications provider may, however, take place on the basis of the provisions regulating the obtaining of correspondence (Art. 236a CCP). These provisions provide for a significantly lower standard under which the authorities conducting criminal proceedings are authorised to obtain content of information they need. In practice, there are cases where the courts accepted the use of rules on interception of telecommunications for acquiring data stored in the cloud (on a virtual drive), which were saved by using the smartphone's function of automatic recording of image and sound in an email inbox, and in this way were constantly in transmission, hence applying a higher standard of protection.[59]

3. Special protection of confidential communications' content

The Polish law of criminal procedure provides special protection for some types of professional secrecy. For example, defence lawyers cannot be questioned as to the facts they learned while providing defence counsel. The same applies to priests regarding facts that they learned during confession (Art. 178 CCP) and to the mediator regarding the facts which they learned from the accused or the victim while conducting mediation (Art. 178a CCP). While these situations are always under protection, there are a number of grounds for secrecy which also allow it to be revoked. A witness remaining under the obligation of professional secrecy other than those indicated above may be interviewed only when permission to hear this person as a witness has been issued by the competent court or prosecutor (Art. 180 § 1 CCP) and regarding some types of professional secrets (a notary, attorney, legal adviser, tax adviser, doctor, journalist) only by the court (Art. 180 § 2 CCP). This last category of witnesses may be interviewed only when two conditions are met: it is necessary in the interests of justice and at the same time, if the circumstances of the crime cannot be established on the basis of other evidence.

The law does not provide a specific prohibition on the interception of telecommunications of persons obliged to maintain professional secrecy. The case law considers the defence lawyer to be outside the circle of people who could be subject to interception of communication.[60] The same applies to priest and mediators. This prohibition results from the philosophy of Arts. 178 and 178a CCP with respect to the defence counsel, priest and mediator.[61] The only way to guarantee the real pro-

---

[59] See *J. Kudła, A. Staszak*, Procesowa i operacyjna kontrola, pp. 55–56.

[60] See Decision of Supreme Court of 26 October 2011, I KZP 12/11, OSNKW 2011, No. 10, pos. 90.

[61] See *K. Dudka*, Kontrola korespondencji i podsłuch w polskim procesie karnym, Lublin 1998, pp. 78–79; *G. Musialik*, Dopuszczalność stosowania podsłuchu telekomunikacyjnego w stosunku do osób zobowiązanych do zachowania tajemnicy zawodowej na gruncie Kodeksu postępowania karnego z 1997 roku, Palestra 1998, No. 11–12, pp. 91–94;

tection of secrecy of defence counselling is an unconditional prohibition on infringing the confidentiality of contact between the accused and the defence lawyer, thus a prohibition on interception of communication between the defendant and the defence lawyer. In relation to persons who are obliged by their profession to keep certain information secret, but where protection is conditional, it is considered that there is no justification to introduce an absolute ban on interception of the content of telecommunications.[62] Interception with regard to persons indicated in Art. 180 § 2 CCP is admissible on an exceptional basis, if the given facts cannot be established on the basis of other evidence. Another view points out that there are no statutory restrictions on intercepting the content of telecommunications regarding persons indicated in Art. 180 § 2 CCP. The use of intercepted data as evidence is admissible only when the provisions of Art. 180 § 2 CCP are met. Pursuant to Art. 226 CCP the provisions of Art. 180 CCP are applied to documents containing professional secrets, and intercepted data should be considered as a 'document' in the meaning of the provisions of the CCP.[63]

The Constitutional Tribunal has concluded – with regard to operational control activities, but it mutatis mutandis applies also to the interception of communication regulated by the CCP – that a general protection from the interception of communication for persons obliged under law to maintain professional secrecy, and even exclusion of information considered to constitute professional secrecy, as strictly unacceptable to obtain in this mode, would lead to significant difficulties in gathering evidence of certain types of crimes, committed, for example, using new technologies. In the Court's opinion, however, it is important to provide appropriate procedural guarantees, eliminating the risk of unauthorised acquisition of information by the Police, which – due to its content and the circumstances of the transfer – should be protected by law. In view of the court, it is essential that there be an effective mechanism enabling an immediate, official and documented destruction of materials containing professional secrets, which do not include information allowing the initiation or conducting of criminal proceedings due to not being useful from the point of view of further proceedings or inadmissible (no legal possibility of their use in further process activities).[64]

There are also no provisions regarding interception of communication carried out by persons covered by formal immunity (e.g., parliamentary deputies, judges). The doctrine presents the position that intercepting the data of such persons is possible only where this does not constitute prosecution of that person, i.e., when they are

---

M. Rusinek, Tajemnica zawodowa i jej ochrona w polskim procesie karnym, Warszawa 2007, p. 209.

[62] *K. Dudka*, Kontrola korespondencji, pp. 77–78; *G. Musialik*, Dopuszczalność stosowania podsłuchu, pp. 89–91.

[63] *M. Rusinek*, Tajemnica, pp. 207–209.

[64] Judgment of Constitutional Court of 30 July 2014, K 23/11, OTK-A 2014, No. 7, pos. 80.

not suspected of committing the offence which is the subject of the proceedings or are only the interlocutor of the person to whom the interception of telecommunications applies.[65]

Polish criminal procedural law does not provide specific safeguards excluding communication in a "core area of private life" from electronic communication interception. The assessment of the admissibility of interception of information such as prayers, communication during sexual activities, diaries, etc. may only be taken into consideration through the constitutional principle of proportionality.

There are also no explicit rules applicable when the intercepted information is privileged, in particular there are no provisions obliging the authorities conducting criminal proceedings to immediately erase this information. It cannot be used in the process as evidence.

4. Execution of telecommunication interception

The provisions of the CCP do not precisely determine how the interception of telecommunications should be executed. Decisions of the court or the prosecutor on interception should indicate an agency (e.g., Police or other agency competent to conduct pre-trial proceedings) which is responsible for executing interception on the side of the authorities conducting criminal proceedings.

An outline of an interception follows from the ordinance of the Minister of Justice of 24 June 2003.[66] On the basis of an interception decision telecommunications service providers are obliged to install on their systems software which are necessary to start and end the interception. Specific communications are extracted from the system of telecommunications service provider by the person authorised by the entitled state agency. The second possibility is for the prosecution authorities to independently perform the interception, without any technical support of the provider (e.g., interception of signals of a wireless network). It should be considered admissible, since the statutory provisions do not specify the mode of interception and do not exclude this option.

The CCP provisions do not grant explicit additional competences or investigative measures to the prosecution authorities executing the interception of electronic communication. The CCP does not set clear rules regarding access to premises that are relevant from the perspective of the proceedings being conducted (e.g., the crime scene). The Constitution guarantees in Art. 50 the inviolability of the home,

---

[65] See *S. Steinborn*, O zakresie ochrony immunitetowej w postępowaniu karnym, in: M. Kłopocka-Jasińska, M. Filipowska-Tuthill (eds.), Immunitet parlamentarny i immunitet głowy państwa z perspektywy konstytucyjnej i karnoprocesowej, Warszawa 2018, pp. 90–92; *K Dudka*, Kontrola korespondencji, pp. 26–27, 78; *B. Janusz-Pohl*, Immunitety w polskim postępowaniu karnym, Warszawa 2009, pp. 245–246.

[66] See footnote 57.

and thus a search of a home, room or vehicle may take place only in the cases specified in the law. Clandestine access to houses, vehicles, etc. in order to place equipment necessary to execute an interception infringe the right to privacy and the inviolability of home and therefore should have an explicit statutory basis. From this perspective it should be seen as inadmissible.

There are also no statutory rules regarding the use of hacking techniques. This means an interference in a computer system. When such computer belongs to a natural person it could also be seen as an infringement of the right of privacy and therefore needs a statutory basis.

5. Telecommunication service providers' duties to cooperate

Duties of the telecommunications entities to cooperate with the prosecution authorities are embedded in the CPP and in the Telecommunications Act.[67] The former is relatively general. According to Art. 237 § 5 CCP, offices, institutions and entities operating in the telecommunications business are obliged to facilitate the enforcement of court or prosecutor decisions on interception of the contents of telecommunications, and to register the conduct of such an interception. However, this obligation is limited only to the situation when the entity mentioned in Art. 237 § 5 CCP operates (uses) the telecommunications network.[68] It means that all providers of telecommunications services are obliged to design their network in such a way that allows the interception of telecommunication. The provisions of the ordinance of the Minister of Justice of 24 June 2003 extend this obligation also to operators who provide telecommunications services while operating a telecommunications network of another operator (so-called MVNO – mobile virtual network operator).[69] The scope of obliged internet providers is wide and includes not only infrastructure providers working on the IP-transport level (such as central network nodes without direct contacts to the users) and access providers on the IP-transport level, but also providers working on the IP-application level providing social interaction (e.g., email or phone services, social networks) or data storing/processing services (e.g., cloud-providers or IoT services, e.g., data transmitted from sensors).

In order to comply with the above requirement, obliged entities shall ensure the technical ability to perform the interception, which in particular implies creating a technical system for interception and recording of transfers of information and storing and destroying records from these transfers, including traffic data. The intercepted transfers of information are saved in such a way that allows them to be ac-

---

[67] Telecommunications Act of 16 July 2004 *(ustawa z 16.7.2004 r. – Prawo telekomunikacyjne)*, Journal of Laws of the Republic of Poland 2018, pos. 1954.

[68] *M. Rogalski*, in: M. Rogalski (ed.), Prawo telekomunikacyjne. Komentarz, Warszawa 2010, Art. 179, sec. 19.

[69] *M. Rogalski*, in: M. Rogalski (ed.), Prawo, Art. 179, sec. 19.

cessed using standard devices. The record is saved on a standard carrier (e.g., CD), together with relevant information identifying this carrier and the criminal case in question. The person (authorised by the competent agency) who performs the interception makes an official note. The carrier and the note are appropriately packaged and then forwarded to the authority that ordered the interception. These activities should be performed in the manner provided for the transmission of messages constituting secret information.

The Telecommunications Act also imposes on telecommunication providers obligations to ensure the possibility of interception of telecommunications. These providers include entities that carry out business consisting of the provision of telecommunications networks, the provision of associated services or the provision of telecommunications services.

Pursuant to Art. 179 (3) Telecommunications Act, telecommunications entities are obliged to provide technical and organisational conditions for access and recording, enabling simultaneous and mutually independent:

1. accessing by the Police and other prosecution authorities of transfers of telecommunications, transmitted or received by the end-user or telecommunications terminal device and data relating to telecommunications transfers held by the telecommunications entity, regarding the user, traffic and location data,
2. obtaining by the prosecution authorities data relating to the telecommunications service provided and user data,
3. recording of telecommunications and data by authorised entities.

Telecommunications entities are also obliged to record those transfers and data for the court and prosecutor. Access to telecommunications transfers and data shall be provided through direct access of the competent authority to the network of the obliged entity, without the participation of its employees. Only telecommunications entities operating on a very small scale are released from this obligation.

Concerning bearing of the costs, pursuant to Art. 179 (3a) and (3b) Telecommunications Act, telecommunications entities are obliged to provide, at their own cost, conditions for access and recording of all offered telecommunications services, and the recording for the court or the state prosecutor of all telecommunications transmissions and data specified in the law.[70] The costs of providing these transfers and data to the courts and prosecutors are borne by the obliged entities.[71]

There is no regulation stipulating technical aspects of the internet provider's transfer of intercepted data to authorities in a foreign country.

---

[70] See *M. Rogalski*, Obowiązki przedsiębiorców telekomunikacyjnych na rzecz obronności i bezpieczeństwa państwa, Prokuratura i Prawo 2007, No. 12, pp. 18 ff.

[71] Decision of Supreme Court of 25 March 2010, I KZP 37/09, OSNKW 2010, No. 5, Pos. 43.

6. Formal prerequisites of interception orders

Pursuant to Art. 237 § 1 CCP, interception of telecommunications may be ordered in principle only by the court, which has the jurisdiction to examine the case in the first instance (Art. 329 § 1 CCP), and only upon application by the public prosecutor.

In emergency cases, the interception of telecommunications may be ordered by the public prosecutor, who is obliged to submit – within three days – a request to the court for authorisation of their decision. The court issues a decision on the request within five days, during a session without participation of the parties (Art. 237 § 2 CCP). According to the case law the 3-day deadline for the prosecutor is an absolute one, which means that not complying with it has the same consequences as not obtaining the court's authorisation.[72] If the public prosecutor does not submit the request for authorisation of interception to the court within this timeframe, the interception of contents of telecommunications must be stopped and information gathered up to that point shall be destroyed. In the opinion of the majority of commentators the court's 5-day deadline is of an instructional nature as otherwise the interception ordered by the prosecutor under Art. 237 § 2 CCP would be ineffective.[73] It means that authorisation of the prosecutor's decision by the court after the 5-day deadline has passed is also valid from the date that the prosecutor's request was received by the court. If the court does not authorise the prosecutor's decision, the intercepted data must be destroyed (Art. 237 § 2 CCP).

There are no special formal requirements for the prosecutor's application, in either common or urgent cases. This application – as a normal procedural motion – should be written and delivered to the court with all investigation files. The application should, however, be justified, and therefore indicate the purpose of the interception, the person against whom interception is to be directed and the period for which it shall be applied.

---

[72] Judgment of Supreme Court of 3 December 2008, V KK 195/08, OSNKW 2009, No. 2, pos. 17; Decision of Supreme Court of 25 March 2010, I KZP 2/10, OSNKW 2010, No. 5, pos. 42.

[73] *T. Grzegorczyk*, Kodeks postępowania karnego. Komentarz, Warszawa 2008, p. 520; *K. Dudka*, Kontrola, p. 69; *R.A. Stefański*, in: Z. Gostyński, R.A. Stefański, S. Żabłocki (eds.), Kodeks postępowania karnego. Komentarz, Warszawa 2004, vol. 1, p. 1019; *W. Grzeszczyk*, Kodeks postępowania karnego, Komentarz, Warszawa 2008, p. 231; *K. Boratyńska, P. Czarnecki*, in: A. Sakowicz (ed.), Kodeks postępowania karnego. Komentarz, Warszawa 2018, p. 640; *J. Grajewski, S. Steinborn*, in: L.K. Paprzycki (ed.), Kodeks postępowania karnego. Komentarz, Warszawa 2013, vol. 1, p. 751; otherwise *P. Hofmański, E. Sadzik, K. Zgryzek*, Kodeks, vol. 1, p. 1297; *J. Skorupka*, Krytycznie o stanowisku Sądu Najwyższego w kwestii legalności kontroli rozmów telefonicznych, Prokuratura i Prawo 2011, No. 4, p. 5.

A decision on the interception of telecommunications shall indicate, as far as is possible,[74] the person against whom the interception is to be directed, the telephone number or the IP-address as well as the period of application of this measure.[75] The interception order should precisely specify the case in which it is ordered. This means that it shall indicate the offence the suspicion of which is the reason for the interception; this offence must be included in the catalogue indicated in Art. 237 § 3 CCP. The decision must be reasoned.

7. Substantive prerequisites of interception orders

Interception of the contents of telecommunications on the basis of the provisions of CCP may be ordered after the investigation has been officially initiated. According to Art. 237 § 1 CCP the interception should be ordered with the aim of detecting and obtaining evidence to be used in the criminal proceedings for which it was undertaken or in order to prevent a new offence.

Art. 237 § 3 CCP determines a list of offences in respect of which interception may be ordered. Recently, however, the legislator has been broadening this list noticeably. No specific degree of suspicion is required. In view of that, the general prerequisite for initiation of criminal proceedings should be applied, which requires a reasonable suspicion of the commission of the offence (Art. 303 § 1 CCP). The potential or the likely sentencing range is of no importance in the process of deciding on the interception.

As for the personal scope of the interception of the contents of telecommunications, it may be ordered against the suspect, the accused and also the injured party (victim) or another person whom the accused may contact or who might be connected with the offender or with the potential offence (Art. 237 § 4 CCP). The list of persons indicated in this provision suggests that a legal person cannot be subject to an interception order. The interception order for the purpose of a criminal investigation should always indicate person against whom it is directed. The interception order is required even if one of the parties to the communication has consented to the interception. It is not possible to direct interception towards particular communication content without specifying the person(s) concerned.

The CCP does not contain an obligation for the court to verify that the interception is proportionate to the seriousness of the offence in the individual case. Such obligation may be however be derived from the constitutional principle of proportionality. For that reason, the court shall consider, *inter alia*, whether other means of investigation less intrusive than electronic communication interception are likely

---

[74] Judgment of Supreme Court of 3 December 2008, V KK 195/08, OSNKW 2009, No. 2, pos. 17.

[75] *K. Eichstaedt*, in: D. Świecki (ed.), Kodeks postępowania karnego. Komentarz, Warszawa 2018, vol. 1, p. 865.

to be successful. As this is not a statutory requirement, in practice consideration for the principle of proportionality is not often given.

There is also no specific requirement regarding the likelihood that the anticipated evidence will actually be obtained by means of the requested interception.

8. Validity of an interception order

Pursuant to Art. 238 § 1 CCP, the interception of telecommunications' content can be ordered for a period not exceeding three months, with the possibility to extend, in particularly justified cases, for a period not exceeding a further three months. The duration of the interception can be prolonged more than once, but its entire duration must not exceed 6 months. An extension of an interception order follows the same procedure as the initial application for an interception.

In case of emergency, the interception can be carried out until the court decides on authorisation of the interception ordered by the public prosecutor, provided that the prosecutor submitted a request to the court for authorisation of the order within three days of the initiation of interception.

Art. 238 § 2 CCP stipulates that the interception be ended immediately after the reasons for it having been ordered cease to exist and at the latest at the end of the period for which it was instituted. This provision means that the court which authorised the interception, or an authority conducting pre-trial proceedings, during which the interception is applied, are under the obligation to continually examine whether the substantive prerequisites of the interception remain valid. In such a situation the interception may also be halted by the authority conducting pre-trial proceedings (e.g., public prosecutor). According to the same line of reasoning, the interception should be terminated if it turns out that the reasons justifying the interception have never really existed. However, this is not necessary if the interception reveals offences which were not initially included in the order.

9. Duties to record, report, and destroy

a) Duty to record and report

Pursuant to the provisions of Ordinance of 24 June 2003, the person conducting the interception prepares a report including in it basic information on the activities. This report is then delivered together with the records of the intercepted material to the court or to the public prosecutor. Neither the provisions of the CCP nor of the Ordinance provide for any obligation to submit reports on the progress of interception.

Pursuant to Art. 237 § 6 CCP, only the court or the public prosecutor are entitled to get acquainted with the content of the recordings, and in urgent cases also the

Police subject to the approval of the court or the public prosecutor. The public prosecutor is entitled to acquaint him/herself with the register of telephone conversation surveillance in the course of preparatory proceedings (Art. 237 § 7 CCP).

b) Duty to destroy

If the records contain information that is entirely without relevance to the criminal proceedings, the public prosecutor shall submit a motion after interception has ended, requiring that all recordings be destroyed (Art. 238 § 3 CCP). The decision on this motion shall be taken by a court without delay, in a hearing without participation of the parties.

If only part of the recording is irrelevant to the criminal proceedings for which the interception was ordered, the public prosecutor shall submit a motion to destroy that part of the recording, provided that this recording does not constitute evidence of another offence. This can be done after the conclusion of the pre-trial phase (Art. 238 § 4 CCP). The court decides on the motion in a hearing which the parties may attend.

A request for the destruction of records may also be submitted after the conclusion of the pre-trial proceedings by the person against whom the interception was ordered (Art. 238 § 5 CCP). The court decides on this request in a hearing, which the parties and the petitioner may attend.

10. Notification duties and remedies

As a rule, decisions issued during pre-trial proceedings that may be subject to interlocutory appeal have to be delivered to the parties. However, as this may jeopardise the whole purpose of the interception, Art. 239 CCP allows the authorities to postpone the delivery of the interception order to the person concerned for a specified period. In the pre-trial proceedings the delivery of the order may be postponed no longer than until the final completion of these proceedings.[76] If interception of contents of telecommunications is ordered against a suspect who has a defence lawyer, this postponement applies also to them. The statutory provisions provide for no obligation to inform the persons whose transfers of data (e.g., phone conversations) have been intercepted immediately after the end of interception.[77] Therefore, it is possible to conduct interception of contents of telecommunications in a completely covert manner throughout the whole period of application of the meas-

---

[76] See also *K. Ponikwia*, Uwagi krytyczne do Art. 239 k.p.k., Prokuratura i Prawo 2002, No. 10, p. 142.

[77] See *P. Hofmański, E. Sadzik, K. Zgryzek*, Kodeks, vol. 1, pp. 1315–1316; *J. Grajewski, S. Steinborn*, in: L.K. Paprzycki (ed.), Kodeks, vol. 1, p. 761; *S. Waltoś, P. Hofmański*, Proces karny. Zarys systemu, Warszawa 2018, p. 386; *T. Grzegorczyk*, Kodeks, p. 520.

ure. The postponement of notification of the indicated persons concerning the interception order is, in practice, a rule.

A court decision regarding interception of contents of telecommunications (not only in the matter of ordering such interception, but also authorising the interception ordered by the public prosecutor, extending the interception's duration, refusing to order the interception) can be subject to appeal to a court of higher instance by any person whom this decision affects (Art. 240 CCP). The decision of the public prosecutor, ordering interception in an emergency situation may be appealed to the court competent to examine the case in first instance (Arts. 240 and 465 § 2 CCP). The appellants may demand in their appeal the examination of factual reasons on which the decision was based as well as its legality. Given the fact that the delivery of the order is usually postponed, in practice the judicial review of the decision occurs after the interception has ended.

An interlocutory appeal against a decision regarding the interception of the contents of telecommunications may be brought not only by the suspect, but also by all persons affected by the interception (e.g., persons living in the same household as the suspect and using the intercepted phone number or computer[78]). The interception order is not formally delivered to such persons, but it would be unfair to deprive them of the possibility to defend their constitutional rights on this basis. According to Art. 302 § 1 CCP a person who is not a party in a criminal proceeding may bring an interlocutory appeal against a decision violating his/her rights.

The appellate review of the decisions regarding the interception of telecommunications is performed according to the general rules.

Abuse of the use of interception against citizens is subject to criminal liability. There is, however, no independent monitoring authority, which has the power to control the interception of communication and is competent to monitor whether it is carried out in accordance with the legal requirements. In that respect citizens have to rely on the prosecutors and judges, independent organisations (e.g., Panoptikon) and their own complaints.

Conducting interceptions illegally or in breach of statutory provisions may be subject to criminal sanctions. It would constitute an offence under Art. 231 § 1 CC, which criminalises acts of public officials going beyond (i.e., abusing) their competences, if it acts to the detriment of the public or private interest.[79] The offence is punishable by imprisonment for up to three years. Potentially the offence of hacking (illegal access to a computer system) could also apply.[80]

---

[78] See *K. Dudka*, Kontrola, p. 86; against *K. Szczechowicz*, Podsłuch telefoniczny w polskim procesie karnym, Olsztyn 2009, p. 66.

[79] *K. Szczechowicz*, Podsłuch, pp. 164–166.

[80] In accordance with Art. 266 §§ 1 and 3 CC, a person who without permission obtains access to information not intended for him or her, connecting to the telecommunications

Interestingly, it results from the above that it is possible that the public official be held criminally responsible for gathering evidence illegally, yet the evidence still be admissible in court. Some authors consider that there is no paradox in that as sanctioning of the official is systemically sufficient.[81] One can, however, question whether this is an acceptable solution from the perspective of legality of the execution of state power.

11. Confidentiality requirements

Pursuant to § 4 of the Ordinance of 24 June 2003, activities related to the execution of orders regarding the interception of information transfers, as well as related deliveries, should be done in the manner provided for the transmission of messages, which have to be protected as classified information constituting a state secret. According to provisions of the Ordinance of 24 June 2003, the data carrier which contains the recording, together with data on transfers and the final report, are packaged in a way preventing access of other persons to the package's content and this package is marked with the case file number. It is then delivered by the authorised agency to the authority which ordered the interception. There are no specific sanctions for infringements of these obligations. However, it may constitute a violation of state secrecy, which is an offence penalised under Art. 266 § 1 CC.

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

a) Relevant provisions

Article 218

§ 1. Offices, institutions and entities conducting postal and telecommunication activity, customs-fiscal offices and transportation institutions and enterprises, are obliged to surrender to the court or the prosecutor, on a demand expressed in decision, any correspondence or packages referred to in Article 180c and 180d of the Act of 16 July 2004 Telecommunications Law, if they are relevant to conducted proceedings. Only the court or the prosecutor may open them or order them opened.

§ 2. The decision referred to in § 1 is served upon the addressee of the correspondence, to the owner of the telephone number or to the sender, whose list of communications or other transmissions of information was surrendered. The service of the decision may be adjourned for a defined period essential to the interests of the case, yet no longer than until the proceedings are validly concluded.

---

network or breaking or bypassing electronic, magnetic, informatic or other specific safeguard, as well as person, who in order to obtain information to which he is not entitled, establishes or uses a tapping device, a visual device or other device or software, is punishable with a fine, community work or imprisonment of up to two years.

[81] See, *inter alia*, *R. Kmiecik*, Kontrowersyjne unormowania w znowelizowanym kodeksie postępowania karnego, Prokuratura i Prawo 2015, No. 1-2, pp. 18–19.

§ 3. Any correspondence irrelevant to criminal proceedings shall be immediately returned to the appropriate offices, institutions or enterprises mentioned under § 1.

Article 218a

§ 1. Offices, institutions and entities conducting postal and telecommunication activity are obliged, upon the request of the court or the prosecutor expressed in a decision, to immediately secure, for a definite period not exceeding 90 days, electronic data stored on hardware devices in IT-systems or on storage media. Article 218 § 2 second sentence applies respectively.

§ 2. The electronic data referred to in § 1, which are irrelevant for criminal proceedings, should be released from seizure immediately.

Article 236a

The provisions of this chapter [Chapter 25 – Search and seizure] apply respectively to the holder and user of a device containing electronic data or of an IT-system, with regard to the data stored on this device or in this system or on a data storage medium in their possession or use, including correspondence sent by e-mail.

b) Requirements for accessing subscriber and traffic data

Pursuant to Art. 218 § 1 CCP, telecommunications providers are obliged on request of the court or public prosecutor to surrender subscriber and traffic data (indicated in detail in Arts. 180c and 180d Telecommunications Act) from their telecommunications network (Art. 218 CCP). This obligation includes the following data:

– data necessary to determine the ending of the network and the telecommunications terminal device, end-user who initiated the connection and to which the connection was routed (for internet connection these are primarily: user-ID, name, surname and address of end-user, IP-address, ID of the digital DSL line, number of network port or MAC-address of the terminal device[82]),
– date and time of the connection and its duration, as well as data regarding unsuccessful connection attempts (by internet access it is date and time of connection and disconnection, as well as attributed dynamic or static IP-address and user-ID[83]),
– type of connection (e.g., landline call, mobile call, SMS, MMS, internet connection[84]),
– location of the telecommunications terminal device (e.g., by mobile phone it is the ID of the BTS station antenna at the time when the call was initiated or re-

---

[82] *M. Rogalski*, Kontrola, p. 86.

[83] *M. Rogalski*, Kontrola, p. 87.

[84] *M. Rogalski*, Kontrola, p. 87.

ceived, geographical coordinates of BTS station, in which area a telecommunication terminal device was located[85]).

The main prerequisite for requesting the subscriber and traffic data is its relevance for an ongoing criminal proceeding (at an investigation or trial phase). The threshold to request the data is suspicion of an offence. It has been pointed out in the literature that this threshold is formulated broadly and does not offer a proper guarantee for what is still a significant interference in the right to privacy. It is therefore proposed that each decision taken on the basis of the indicated regulation should always be carefully examined.[86] The relevance of the requested data for the ongoing criminal proceedings shall be examined *ex ante* – before the decision to request this data is taken, and then *ex post* – after data is obtained by the court or public prosecutor.[87] As to the latter, if it becomes clear that the data obtained is irrelevant for the criminal proceedings for which it was gathered, it shall be immediately returned to the appropriate telecommunications provider (Art. 218 § 3 CCP).

Provisions of the CCP do not provide the possibility to access subscriber and traffic data by way of an automated online procedure. The authority therefore has to always rely on cooperation with the telecommunications providers.

The request for subscriber and traffic data is addressed to the telecommunications provider. This request must be based on a decision of the court or public prosecutor. The decision requesting the data has to be delivered to the subscriber concerned. However, the delivery of the decision may be postponed for a specified period, and only as long as it is necessary, but not for longer than until the final conclusion of proceedings (Art. 218 § 2 CCP).

The law offers the possibility of judicial review of the requests for subscriber and traffic data. The decision requesting the data may be appealed to the county court by persons whose rights have been violated (Art. 236 CCP). Decisions taken by the public prosecutor may be appealed to the county court on whose territory the pre-trial proceedings are conducted. It is possible that the decision requesting the data will be reviewed at a relatively late stage of proceedings, even after the final conclusion of criminal proceedings, since then the person concerned has obtained the information on the request. The review in such a case is independent from the normal course of proceedings.

Only the court and the public prosecutor have the right to inspect or to order the inspection of the obtained data (Art. 218 § 1 CCP). If such order is issued by the prosecutor, the data could be inspected by the agency conducting pre-trial proceed-

---

[85] *M. Rogalski*, Kontrola, pp. 87–88.

[86] *P. Hofmański, E. Sadzik, K. Zgryzek*, Kodeks, vol. 1, p. 1230.

[87] *M. Rogalski*, Kontrola, pp. 91–92; *P. Hofmański, E. Sadzik, K. Zgryzek*, Kodeks, vol. 1, p. 1233.

ings (e.g., the Police). A written record is drawn up of the inspection of obtained data (Art. 143 § 1 (7) CCP).

The CCP also offers rules on freezing traffic and subscriber (as well as content) data. Pursuant to Art. 218a § 1 CCP, at the written request of the public prosecutor telecommunications entities are obliged to immediately secure computer data stored in devices containing this data, on a data carrier or in an IT system. Data may remain frozen for a definite time period not exceeding 90 days. This decision may also be appealed and the same rules on delivery of decision and judicial review apply as for access to the data.

c) Telecommunication data retention

Pursuant to Art. 180a section 1 Telecommunications Act, operators of the public telecommunications network and providers of publicly accessed telecommunications services are obliged to retain subscriber information and traffic data indicated by Art. 180c Telecommunications Act. This data shall be stored for 12 months from the day of connection or unsuccessful attempt at connection. The period of the retention is calculated for each piece of data separately.[88] Stored data include:

– data necessary to determine the ending of the network and the telecommunications terminal device, end-user who initiated the connection and to which the connection was routed,
– date and time of a connection and its duration,
– type of connection,
– location of the telecommunications terminal device.

Regarding internet connections retained data includes: user-ID; number attributed to the end-user using dial-up access; user-ID and number attributed to the end-user initiating connection to the public telecommunication network, IP-address; name, surname (or name of entity) and address of the end-user, whose IP-address was attributed during connection, as well as user-ID or number attributed in VoIP-service; end of network-ID, where user accessed the internet, especially DSL-ID, number of the used network-port, MAC-address of the terminal device, which initiated connection; date and time of each internet connection and disconnection according to local time, with dynamic or static attributed IP-addresses used during connection and user-ID; date and time of login and logout to the email service and VoIP-service, according to local time.[89]

---

[88] *M. Rogalski*, Kontrola, p. 292.

[89] The precise list of retained data is provided for by the Ordinance of Minister of Infrastructure of 28 December 2009 (Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług tele-

In addition, it should be noted that the Telecommunications Act provides for two independent legal bases for storing and making available subscriber and traffic data. The first one is Art. 180c, which concerns data which is required to be retained for a period of 12 months. The second basis is Art. 180d, which provides for the obligation to make available data relating to the service offered by service providers that operators process for their own use. This type of data largely coincides with that referred to in Art. 180c.

The obligation to provide data at the request of a court or a prosecutor, which is anchored in Art. 218 § 1 CCP in conjunction with Art. 180d Telecommunications Act, is not limited in time. Therefore, that obligation can be considered to exist for the entire period during which the data is being stored by the service provider, that is to say, also after the 12-month period of obligatory retention is over. This would lead to the conclusion that the service provider may not refuse to make data available after a period of 12 months, even if the data is that referred to in Arts. 180a and 180c Telecommunications Act, if the data is processed by the service provider in connection with the provision of a telecommunications service. However, the doctrine considers that the storage of data by the provider of telecommunications services for a period longer than 12 months is allowed only in cases provided for in the Telecommunications Act and only for the purpose specified in these regulations (e.g., for the purposes of proceedings resulting from customer's complaint). For the purposes of criminal proceedings, the data shall be stored pursuant to Art. 180a Telecommunications Act for a period of 12 months. Therefore, if a court or a public prosecutor asks a telecommunications service provider that retains data of a subscriber for data which coincides with the data referred to in Art. 180c 12 months after the registration of the data in question, the provider should refuse to provide access to that data.[90]

2. Determination of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

According to Art. 180a sec. 1 and Art. 180c Telecommunications Act and provisions of the Ordinance of Minister of Infrastructure of 28 December 2009,[91] telecommunications providers are obliged to retain the following data of mobile phone users, who initiated connection and users to whom connection was directed: MSISDN number, IMSI number, IMEI number of the terminal device, geographical coordinates of BTS station, in which area a telecommunication terminal device was located, as well as azimuth, beam, and working range of the BTS station antenna. This data may be requested by the court and public prosecu-

---

komunikacyjnych obowiązanych do ich zatrzymywania i przechowywania; Journal of Laws of the Republic of Poland 2009, No. 226, pos. 1828).

[90] *M. Rogalski*, Kontrola, pp. 294–297.

[91] See footnote 89.

tor on the basis of Art. 218 § 1 CCP. There are no particular rules as regards these categories of data.

D. Access to (Temporarily) Stored Communication Data

1. Online-searches by means of so-called remote forensic software

Polish law does not contain provisions in respect to online search of computers and such a measure is at present inadmissible.[92] The Ministry of Internal Affairs and Administration prepared in 2010 a draft regulation on online search of computers as an operational and exploratory activity conducted by the Police, but the work on it has been discontinued. For that reason, and in accordance with the principle of legality, any sort of hacking committed by the Police or other authorities for preventative purposes is not permitted.

2. Search and seizure of stored communication data

Polish criminal procedure does not contain specific rules with respect to searches for stored communication data. Pursuant to Art. 236a CCP, the provisions on search of premises can be applied to a search of a device containing IT data (e.g., computer) or an IT system (e.g., computer network) with respect to data stored on that device, in that system or on a data carrier (e.g., DVD, USB), including correspondence sent by email. On that basis, provisions regarding the person whose premises are searched are applied accordingly to the holder and user of the given device, carrier or IT system. This legislative technique raises many theoretical and practical problems as the provisions written for the search of premises and seizure of objects do not take into account the specificity of the search of IT systems and seizure of electronic data. The following paragraphs give an account of the rules as they are being interpreted from the general provisions on search and seizure.

Search of devices, carriers and systems may be conducted in order to find data that might serve as evidence in a concrete criminal proceeding, provided that there are justified reasons to believe that the device, carrier or system contains communication data. The use of these provisions is not limited to a certain category of offences. The given device, carrier or IT system may belong to or be used by the suspect, but may very well belong to another person.

A search must be ordered with a written reasoned decision of the court (during trial phase) or of the public prosecutor (during pre-trial phase) and may be conducted by a public prosecutor, the Police or another investigative authority (e.g., The Internal Security Agency).

---

[92] See *A. Lach*, Przeszukanie na odległość systemu informatycznego, Prokuratura i Prawo 2011, No. 9, p. 67.

If the data is being sought on a computer or storage device, it is common practice that the competent authority seizes the computer or the device and the device is examined by an expert in order to find the requested data. The doctrine considers this practice to be disproportionate as the owner is deprived of its use for months or even years. It is hence argued in the literature that seizure of stored data should mean copying this data and seizure of the device should only be applied if it was also an instrument of crime.[93]

The law offers the possibility – in urgent cases – to conduct search by the Police or an authorised agency upon presentation of a warrant issued by the head of the responsible unit of the authority performing the search, or an official ID of the person conducting the search (Art. 220 § 3 CCP). After performing the search, the authority that performed the search must immediately request the public prosecutor's authorisation. The prosecutor's decision authorising the search must be delivered to the owner or the user of the device, carrier or IT system within 7 days from the date of the search, provided that that person so requested. The person should be informed of his/her right to make the request. In practice, the above described practice of conducting a search without the court's or prosecutor's order is common, and the prosecutors provide subsequent authorisations almost automatically.

The law offers to the persons whose rights were violated the possibility of judicial review of the decisions described above as well as of the manner in which the search was conducted.

Polish law guarantees a lower level of protection when conducting access to and seizure of stored data than for interception of content of telecommunications while in transmission. This is clearly visible with respect to correspondence sent by email. Interception of these communication while they are being transmitted ("live") is subject to provisions on the interception of telecommunications (chapter 26 of CCP) and therefore requires a court decision; it can only be applied to more serious offences and for a specific period of time. However, if this correspondence is saved on a device (e.g., the addressee's computer) or in the IT system (e.g., on an email server or in the cloud), access to them is subject to provisions on seizure of correspondence.[94] In accordance to these rules the stored data may be obtained with regard to any offence with only a decision of the public prosecutor without involvement of the court (not to mention the practice of subsequent prosecutor's order). In order for the authorities to use this provision it is not even necessary that the message reach the addressee. It is also possible to seize it immediately if at the moment of seizure the data is temporarily stored (before or after sending).[95]

---

[93] *A. Lach*, Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego, Prokuratura i Prawo 2013, No. 10, p. 22.

[94] See *P. Hofmański, E. Sadzik, K. Zgryzek*, Kodeks, vol. 1, p. 1232; *M. Rogalski*, Kontrola, pp. 101–102.

[95] *A. Lach*, Gromadzenie, p. 19.

The search of a computer, another device or an IT system containing communications data is performed as an open measure. There is no obligation to provide prior notification of a planned search, neither to the suspect, nor to the person whose device is to be searched or to the provider of the IT system. There is no possibility for conducting a clandestine search in the absence of any persons, because the right to be present during the search is granted to persons whose device or IT system is to be searched and a person designated by them, if this does not obstruct the search or render it impossible. If the owner of the device or IT system is not present during the search, at least one adult member of the household, a neighbour or employee of the owner should be called to attend.

Access to stored communications data can also be obtained in a clandestine way. Pursuant to Art. 218 § 1 CCP, telecommunications providers are obliged on request of the court or public prosecutor to produce correspondence. This provision is applied accordingly to seizure of correspondence sent by email, stored in a cloud or server of email. Delivery of the court or prosecutor decisions concerning that production order or seizure to the person concerned may be withheld for a specified period, necessary for the proper conduct of the case, but not longer than until the final conclusion of proceedings. In such a situation, seizure of the data is in fact performed in a clandestine way.

3. Duties to cooperate: production and decryption of data

Providers of telecommunications services pursuant to Art. 218 CCP are obliged upon request of the court or the public prosecutor to produce subscriber and traffic data (see above C.1.a.–b.).

The Code of Criminal Procedure does not provide for any special rules on which the investigative authorities could request the decryption of encrypted data or the surrender of the passwords necessary for decryption. Data necessary for decryption may be obtained only upon general rules concerning duties of witnesses. Interrogated witnesses shall give truthful testimony under threat of criminal responsibility (Art. 233 CC), and therefore also give information necessary for decryption, if they have relevant knowledge. The provisions regulating obligations of the custodian of objects in cases of search and seizure do not foresee any obligation to surrender encryption data. Such person has only the obligation to endure the activity of the authority conducting the search.[96] The accused persons also do not have such an obligation, because pursuant to Art. 74 § 1 CCP and the rule of *nemo tenetur* they are not obliged to provide evidence to their disadvantage.

---

[96] *A. Lach*, Gromadzenie, p. 21; *M. Rogalski*, Kontrola, p. 127.

IV. Use of Electronic Communication Data in Judicial Proceedings

1. Use of electronic communication data in the law of criminal procedure

There are no specific rules in Polish criminal procedure for using intercepted electronic communications data in court proceedings.

Audio recordings of tapped conversations and other transmissions of information (see above B.2.a.) are treated like documents and follow the same rules of the Code of Criminal Procedure. According to current case law, the inclusion of audio recordings of previously recorded telephone conversations as evidence during trial takes place in principle by reproducing these records during the hearing before the court. As an exception to the principle of directness, it is also possible to consider the recording as disclosed without being reproduced, unless the parties present at trial object.[97] Information on the reproduction of a recording or on its disclosure without reproduction must be included in the file and the transcription of the content of the recording is then annexed into the file.[98] In case of doubt or if questioned by the accused person, the interlocutors of the recording shall be identified by an expert.

The content of emails, text messages, subscriber or metadata (data on network traffic) obtained from the telecommunications service providers and any other data obtained in writing (as a document) becomes included in the file as evidence by reading them aloud during trial or by considering them as disclosed without reading, in the same way as mentioned in the previous paragraph.[99]

2. Inadmissibility of evidence as a consequence of inappropriate collection

Art. 51 (4) Constitution provides for the right to demand rectification or removal of information collected illegally. On the basis of this provision, the Constitutional Tribunal decided in 2015, that tapped conversations resulting from operation control cannot be retained (i.e., must be destroyed) if they were collected against the law, namely without a court order, even if they could prove the commission of an offence.[100] Art. 51 (4) Constitution is strict in that regard, and the limitation of the right cannot be provided by a statute (the limitation would need to be permitted by

---

[97] Art. 394(2) CCP.

[98] Judgment of Supreme Court of 10 June 2008, III KK 30/08, OSNKW 2008, No. 8, pos. 65; Judgment of Court of Appeal Gdańsk of 17 October 2013, II AKa 208/13, LEX No. 1394173; Judgment of Court of Appeal Białystok of 30 October 2012, II AKa 170/02, LEX No. 1298861; *D. Szumiło-Kulczycka*, Czynności, pp. 184–189.

[99] Art. 394(2) CCP.

[100] Judgment of Constitutional Court of 12 December 2005, K 32/04, OTK-A 2005, No. 11, pos. 132.

the Constitution itself, which is not the case).[101] This judgment thus created a distinction between the illegality of obtaining information about an individual and the illegality of its use.

Illegal acquisition of information should always lead to the inadmissibility of its use.[102] This philosophy has led jurisprudence and doctrine to establish in the first decade of the 21st century that if the statutory conditions for carrying out operational and exploratory activities (e.g., operational control) are not observed, materials collected during these activities are not admissible as evidence at trial.[103] The jurisprudence[104] and the doctrine[105] extended this view to evidence collected in the pre-trial phase upon provisions of CCP (e.g., material collected as a result of wiretapping conducted in the pre-trial phase, but in breach of the statutory conditions provided by the CCP).

However, it is rightly concluded that violations of Art. 51 (4) Constitution, in particular minor violations, do not automatically require that the data gathered be deleted. Since Art. 51(4) Constitution is intended to protect against unjustified and excessive interference in the constitutional rights and freedoms of individuals, what is relevant is precisely the violation of substantive and constitutional conditions for infringing privacy. These conditions include the manner of interference (the type of undertaken activity), the personal, material and temporal scope of the interference and the type of the authority entitled to order or approve the activity. Therefore, violations of regulations of purely organisational or technical character should not result in the inadmissibility of the use of the obtained data as an evidence.[106]

The situation changed significantly on 15 April 2016, when the new provision of Art. 168a CCP entered into force. According to that provision, evidence cannot be considered inadmissible on the sole ground that it was obtained in breach of procedural rules or even by means of a criminal offence (with a few exceptions, such as murder, intentional bodily harm or imprisonment; interestingly, some form of torture without causing bodily harm, or causing it only non-intentionally, would not

---

[101] See also Judgment of Constitutional Court of 26 October 2005, K 31/04, OTK-A 2005, No. 9, pos. 103.

[102] *D. Szumiło-Kulczycka*, Czynności, pp. 142–143.

[103] Decision of Supreme Court of 22 September 2009, III KK 58/09, OSNKW 2010, No. 3, pos. 28; Decision of Supreme Court of 30 November 2010, III KK 152/10, OSNKW 2011, No. 1, pos. 8; Decision of Supreme Court of 19 March 2014, II KK 265/13, OSNKW 2014, No. 9, pos. 71.

[104] Judgment of Supreme Court of 3 December 2008, V KK 195/08, OSNKW 2009, No. 2, pos. 17.

[105] See inter alia *J. Skorupka*, Eliminowanie z procesu karnego dowodu zebranego w sposób sprzeczny z ustawą, Państwo i Prawo 2011, No. 3, p. 80; *D. Drajewicz*, Zakaz dowodowego wykorzystania procesowej kontroli rozmów, Państwo i Prawo 2011, No. 8, pp. 76–77; *D. Szumiło-Kulczycka*, Czynności, pp. 143–144, 367.

[106] *D. Szumiło-Kulczycka*, Czynności, pp. 149–151.

exclude the use of evidence obtained in that way). This provision is considered highly controversial and constitutionally questionable.[107]

It is therefore not clear how the consequences of infringement of regulations specifying the formal and material prerequisites for obtaining telecommunications data should currently be assessed. A number of interpretations have been formulated, all curtailing the potentially worrying impact of the provision on acquisition of evidence. The only difference between them, is extent to which the provision is limited. The most modest interpretation considers that this provision prohibits a court from declaring evidence inadmissible solely on the ground that it was obtained unlawfully, unless it was obtained in connection with the performance of a public official's duties.[108]

Another interpretation points out that, since Art. 168b CCP prohibits declaring evidence inadmissible "merely" on the ground that it was obtained in breach of the law, the provision can be read as requiring that not only the breach be taken into account when declaring evidence to be inadmissible, but that the impact of the procedural irregularity on the evidence in question be examined. Hence, there is no obligation under this provision to use evidence obtained in significant breach of statutory requirements, e.g., exceeding the statutory competence of an authority. The most far-reaching views are those considering that evidence obtained as a result of actions contrary to the law is obtained in an unconstitutional manner and as such should not be used in criminal proceedings at all.[109]

It is this last view that seems to be most pervasive in current jurisprudence. One of the first significant judgments regarding this new provision assumed that evidence obtained in the course of operational control which was ordered by a court, but the scope of which went beyond the legal limitations and was hence contrary to the requirements of the law, cannot be considered to be legal evidence and thus is inadmissible in the proceedings. The rule one can decode from this judgment is that evidence may be considered inadmissible if it was obtained in violation of the rules of procedure or by means of a criminal act and in violation of the provisions of the

---

[107] See, *inter alia*, *P. Wiliński*, Konstytucyjny standard legalności dowodu w procesie karnym, in: S. Steinborn, K. Woźniewski (eds.), Proces karny w dobie przemian. Zagadnienia ogólne, Gdańsk 2018, pp. 314–316; *T. Grzegorczyk*, Kodeksowe legalizowanie w procesie karnym, przez nowelizację z 11 marca 2016 r., dowodów uzyskanych za pomocą przestępstwa lub z naruszeniem przepisów postępowania albo poza granicami zgody udzielonej przez sąd na wkroczenie w sferę konstytucyjnie chronionych wolności jednostki, in: S. Steinborn, K. Woźniewski (eds.), Proces karny w dobie przemian. Zagadnienia ogólne, Gdańsk 2018, pp. 326–328; *R.A. Stefański*, Dowód nielegalny w postępowaniu karnym, in: S. Steinborn, K. Woźniewski (eds.), Proces karny w dobie przemian. Zagadnienia ogólne, Gdańsk 2018, pp. 353–355.

[108] See *D. Gruszecka*, in: J. Skorupka (ed.), Kodeks postępowania karnego. Komentarz, Warszawa 2017, p. 341.

[109] *R.A. Stefański*, Dowód, pp. 354–355; *K. Boratyńska, P. Czarnecki, M. Królikowski*, in: A. Sakowicz (ed.), Kodeks postępowania karnego. Komentarz, Warszawa 2018, pp. 483–484.

Constitution. If these conditions are fulfilled, the statutory restriction expressed in Art. 168a CCP does not restrict the judge's liberty to consider the evidence to be inadmissible.[110]

3. Use of data outside the main proceedings

a) Data from other criminal investigations

In the first years of the 21st century, the jurisprudence adopted the view that evidence from a legally ordered and conducted operational control cannot be used in criminal proceedings for a different offence, if the latter was not included in the list of offences for which the control could be ordered.[111] On the contrary, if the offence is on the list, the evidence gathered during such operation control can be used even in the proceedings against a different person or for a different offence than the person or offence for which the control was originally ordered. In that case the admissibility depends, however, on the court's so-called subsequent (i.e., retrospective) consent.[112]

A similar position was also adopted with regard to wiretapping during criminal proceedings on the basis of the CCP.[113] In 2011, the procedure of granting subsequent consent, which previously was a jurisprudential practice, was explicitly regulated in the provisions of the Law on Police and the CCP.

The same law also included two other changes that, similarly to the former one, embodies case law rules on a statutory basis. Firstly, it added a new paragraph (Art. 237 § 8 CCP), which provided that the use of evidence obtained during the control as well as the recording of the content of telephone conversations is admissible only in criminal proceedings for a criminal offence or fiscal offence against which it is possible to order such control. Secondly, Art. 237a CCP stated that if, as a result of the interception of telecommunications evidence of an offence referred to in Art. 237 § 3 CCP (containing a list of offence to which operational control may be applied) was gathered, but a different offence to that initially mentioned in the order, or the offence was committed by a person other than the one to whom the control was applied, the public prosecutor may in the course of the interception

---

[110] Judgment of Court of Appeal in Wrocław of 27 April 2017, II AKa 213/16, OSA 2017, No. 4, pos. 6.

[111] Decision of Supreme Court of 26 April 2007, I KZP 6/07, OSNKW 2007, No. 5, pos. 37.

[112] Decision of Supreme Court of 26 April 2007, I KZP 6/07, OSNKW 2007, No. 5, pos. 37; Decision of Supreme Court of 23 March 2011, I KZP 32/10, OSNKW 2011, No. 3, pos. 22; see also *D. Szumiło-Kulczycka*, Czynności, pp. 199–200.

[113] Decision of Supreme Court of 25 March 2010, I KZP 2/10, OSNKW 2010, No. 5, pos. 42; see also *K. Szczechowicz*, Podsłuch, pp. 68–69.

or no later than two months from the date of its completion, apply to the court for consent to its use in criminal proceedings.

The situation changed yet again recently with the amendments passed on 11 March 2016, which further extended the use of materials gathered during the interception of conversations and other transfers of information. Art. 237 (8) CCP was outright deleted, while Art. 237a CCP was rewritten. In its new formulation it provides that if, as a result of an interception, evidence of an offence other than that covered by the original order was obtained from a person to whom the control was applied, or evidence of an offence committed by a person other than that covered by the order, then the public prosecutor shall decide on the use of that evidence in criminal proceedings. The only limitation provided for in this provision is the requirement that this new offence be prosecuted *ex officio*. Compared to the previous situation, there is no longer a requirement for a subsequent consent of the court.

This relaxed framework is questionable as regards in particular the possibility to use evidence from wiretapping as to which the use of this measure was not possible at all. The problem stirred significant debate in the literature,[114] and eventually was subject to an analysis by the Supreme Court, even if as regards a different but analogous Art. 168b CCP, which practically reintroduced the rules that existed before the changes of 2016.

The Supreme Court pointed out the ambiguity of the statutory provision and used primarily constitutional argumentation. The constitutional protection of human freedom refers primarily to the sphere of his privacy (protected in Arts. 47 and 51 Constitution). At the same time, it is unacceptable to presume the competence of public authorities to interfere in the freedom of the individual. The constitutional principle of proportionality in particular requires that the legislator define a limited and possibly narrow list of serious crimes justifying operational control that interferes with individual rights, such as privacy. In view of this principle, it is necessary to seek an interpretation of the provisions in question, which would allow the legislator to achieve the set goal when introducing such provisions, and at the same time be the least burdensome for the addressees of legal norms, and in any case will not be more burdensome than necessary to achieve the goal set by the legisla-

---

[114] For the wide interpretation: *K. Eichstaedt*, in: D. Świecki (ed.), Kodeks, vol. 1, pp. 870–871; *T. Grzegorczyk*, Kodeksowe legalizowanie, pp. 334–335; *B. Sitkiewicz*, Wykorzystanie dowodów uzyskanych w ramach kontroli operacyjnej oraz podsłuchu procesowego, in: A. Lach (ed.), Postępowanie karne po nowelizacji z dnia 11 marca 2016 r., Warszawa 2017, pp. 117–119; for the narrow interpretation: *J. Skorupka*, Prokonstytucyjna wykładnia przepisów prawa dowodowego w procesie karnym, in: T. Grzegorczyk, R. Olszewski (eds.), Verba volant, scripta manent. Proces karny, prawo karne skarbowe i prawo wykroczeń po zmianach z lat 2015–2016. Księga pamiątkowa poświęcona Profesor Monice Zbrojewskiej, Warszawa 2017, pp. 363–364; *D. Gruszecka*, in: J. Skorupka (ed.), Kodeks, pp. 346–348.

tor. The conflict between the principle of legality, which is based on the objective of combatting crime, and the principle of respect for and protection of human freedom, must be resolved while respecting the principle of proportionality (Art. 31 (3) Constitution), through strict statutory regulation of situations where public authorities are entitled to interfere with individual freedoms.

As a consequence, the Supreme Court held that in a criminal trial it is possible under Art. 168b CCP to use materials obtained as a result of operational control which relate to an offence other than that for which control was ordered (including as regards another person), only if it is an offence for which operational control was permitted at all.[115] In the same way this issue should be understood under Art. 237a CCP as regards wiretapping.

b) Data from preventive investigations

Data collected in the course of operational and exploratory activities undertaken on the basis of the Police law (e.g., operational control) may be used as evidence in criminal proceedings. From the principle of legality, which also binds the Police, stems an obligation for the Police to use in criminal proceedings all materials obtained in the course of operational and exploratory activities, which are significant for the criminal proceedings.[116] In cases where the pre-trial proceedings are conducted by the public prosecutor, this means an obligation to pass these materials to the prosecutor. These materials can justify the initiation of pre-trial proceedings, and may also be used in already ongoing proceedings.

The statutory regulation regarding the use of these materials is not, however, comprehensive. Pursuant to Art. 19 (15) Law on Police all materials obtained as the result of operational control, when they are relevant for initiation of criminal proceedings or for ongoing criminal proceedings, shall be transferred by the Police to the appropriate public prosecutor. In the course of court proceedings (trial), the materials – pursuant to Art. 393 § 1 CCP – are read aloud or if they are recordings – played.[117] In turn, the question of the use of subscriber and traffic data gathered on the basis of Art. 20c Law on Police has been not clearly regulated. It is assumed that it would be unreasonable, however, to accept the view that the use of these materials is inadmissible. It is pointed out that functional arguments support the use of this data during the criminal proceedings, especially as these materials come not from state agencies, but from third parties (e.g., telecommunications providers).[118]

---

[115] Decision of Supreme Court of 28 June 2018, I KZP 4/18, OSNKW 2018, No. 8, pos. 53.

[116] *A. Taracha*, Czynności, p. 76.

[117] Judgment of Supreme Court of 10 June 2008, III KK 30/08, OSNKW 2008, No. 8, pos. 65.

[118] *D. Szumiło-Kulczycka*, Czynności, pp. 270–271.

Therefore, this data may be used during criminal proceedings following the same rules as data collected during criminal proceedings.

c) Data obtained from foreign jurisdictions

The provisions of the CCP do not contain any specific regulations concerning the use of telecommunications data obtained from another state through mutual legal assistance, but some more general provisions may be of application. The provision of Art. 587 CCP allows the use (pursuant to the rules prescribed by Arts. 389, 391 and 393 CCP) of inspection reports, interviews with persons as defendants, witnesses, experts or minutes of other evidentiary acts performed by courts or prosecutors of foreign countries or by authorities acting under their supervision, provided that the manner of performing these acts is not contrary to the legal order in Poland.

Given the fact that data obtained through wiretapping is to be used as evidence at an oral hearing in accordance with Art. 393 § 1 CCP, the provision of Art. 587 CCP should be regarded as also applying. This leads to the conclusion that the content of data obtained from another country may be used in a criminal proceeding conducted in Poland, if the manner of obtaining such data is not contrary to the principles of the legal order of Poland. Such a position has also been expressed in the case law, indicating that the legality of telephone tapping by foreign authorities in the course of proceedings in a foreign country should be assessed in accordance with the provisions in force in the country where the operation is carried out, while in Poland these materials are subject to assessment pursuant to Art. 587 CCP.[119]

4. Challenging the probity of intercepted data

Data obtained by wiretapping shall be evaluated in the same way as any other type of evidence in criminal proceedings. In practice, however, it is quite difficult to challenge the reliability of intercepted data, as it is obtained from telecommunications service providers, and the parties have no insight into the process of obtaining it, but only have access to a report documenting the interception of data. For this reason it is a general practice that defence counsels question the legality and the admissibility of collected data rather than the way in which it was obtained or the content of the data.

As to recordings of telephone conversations, the identity of recorded persons is most frequently questioned, which makes it necessary to subject the recordings to phonoscopic examination. These are carried out by independent experts. If reasonable doubts are raised as to the reliability of the telecommunications data obtained,

---

[119] Judgment of Supreme Court of 19 September 2000, V KKN 331/00, LEX nr 50992; Judgment of Court of Appeal Katowice of 7 February 2008, II AKa 6/08, LEX nr 399957.

e.g., that the data was altered, subjected to unauthorised selection and does not form an integral whole or was distorted in the course of copying, it is possible to appoint an IT expert to verify these allegations. In exceptional cases, it also seems possible to interview the person who recorded the data as a witness.

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

1. International Conventions

1. The European Convention on MLA in Criminal Matters of 20 April 1959 was signed by Poland on 9 May 1994 and ratified on 19 March 1996.
2. The Convention on MLA in Criminal Matters between the Member States of the EU of 29 May 2000 entered into force on 26 October 2005.
3. The United Nations Convention against Transnational Organized Crime of 15 November 2000 was ratified by Poland in 2001.
4. Finally, the CoE Cybercrime Convention of 23 November 2001 has been signed by Poland on 23 November 2001, but ratified only on 20 February 2015.

2. Bilateral treaties

In general, mutual legal assistance agreements do not contain specific rules on wiretapping and obtaining telecommunications data. However, many of these agreements enable a very wide range of measures to be undertaken, and usually the catalogue of these activities is open. Hence, cooperation in relation to obtaining telecommunications data is not excluded. These agreements usually do not require the double criminality condition, but at the same time they provide for the possibility of refusing cooperation due to the *ordre public* clause or contain a similar solution. For instance, the agreement of 26 February 2004 between the Republic of Poland and the Kingdom of Thailand on mutual assistance in criminal matters provides in Art. 2 (1) for the possibility of refusing to execute a request for assistance if its execution could violate the sovereignty, security or other essential public interest of the requested State.[120] It seems that even without the requirement of dou-

[120] Agreement between the Republic of Poland and the Kingdom of Thailand on mutual assistance in criminal matters, done at Bangkok on 26 February 2004, accessible at http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20092081607/O/D20091607.pdf (last visited October 2019).

ble criminality, assistance regarding wiretapping or exchange of telecommunications data will be refused on that basis.

Poland has signed MLA treaties with the US[121] and Canada.[122] While neither of these treaties contains provisions specifically regarding rules on interception of telecommunications, they provide the legal basis for MLA requests between Poland and these two countries.

In particular, the MLAT with the US provides in: Art. 1 (2) that assistance shall include: b) providing documents, records, and articles of evidence; f) executing requests for searches and seizures; h) any other form of assistance not prohibited by the laws of the requested State.

The MLAT with Canada requests both countries to grant each other the widest measure of mutual legal assistance in criminal matters. Art. 1 (5) provides that legal assistance shall include (c) provision of information, documents and other records; (f) search for and seizure of documents, records or things; (l) other measures consistent with the objects of this Treaty.

Both treaties do not require double criminality.[123]

One may also mention the Agreement on Police Cooperation of 2014 between Poland and Germany, which in its Art. 6 (1) provides for exchange of data on subscribers and users of telecommunication and ICT networks. This agreement is limited only to Police cooperation.[124]

3. National regulation

The implementation of the above instruments and setting out of the framework of cooperation has been done by including, amending and adding several chapters to the CCP, in particular chapters 62, 62a–d, 65.

Chapter 62 sets out a general framework for mutual legal assistance, in particular with regard to relations with third states (non-UE). Chapters 62a–b deal with non-

---

[121] Treaty between the United States of America and the Republic of Poland on Mutual Legal Assistance in Criminal Matters, signed at Washington on 10 July 1996, accessible at https://www.congress.gov/105/cdoc/tdoc12/CDOC-105tdoc12.pdf (last visited October 2019).

[122] Treaty Between Canada and the Republic of Poland on Mutual Legal Assistance in Criminal Matters, signed at Ottawa on 12 September 1994, accessible at https://www.treaty-accord.gc.ca/text-texte.aspx?id=101634 (last visited October 2019).

[123] MLAT with the US: Art. 1 (3), MLAT with Canada: Art. 1 (6).

[124] Agreement between the Government of the Republic of Poland and the Government of the Federal Republic of Germany on cooperation between police, border and customs services, concluded in Zgorzelec on 15 May 2014, accessible at http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20150000939/O/D20150939.pdf (last visited October 2019).

EIO requests with the EU regarding enforcement of a decision to seize evidence or to secure property. Chapter 62c deals with Polish EIO requests and chapter 62d with the EIO requests addressed to the Polish authorities.

None of these provisions deal specifically with interception of communications, with the exception of two provisions regarding the implementation of the European Investigation Order Art. 589zd and Art. 589zt (see below).

B. Requirements and Procedure

1. Incoming requests

Art. 588 CCP constitutes a general legal basis of mutual legal assistance where Poland is the requested State. This article stipulates that courts and prosecutors provide legal assistance at the request of foreign courts and prosecutors, unless the requested act would be contrary to the principles of the legal order of the Republic of Poland or would violate its sovereignty. While Polish law applies, the authorities should strive to satisfy the wishes of requesting authorities concerning special procedures, if it is not contrary to the principles of the legal order.

The court and the prosecutor shall refuse to grant legal aid and transmit the refusal to the competent authorities of a foreign State if the requested action would be contrary to the principles of the legal order of the Republic of Poland or would violate its sovereignty.

Furthermore § 3 of Art. 588 CCP allows the court or the prosecutor to refuse providing legal assistance if:

1. the performance of the requested action does not fall within the scope of activity of the court or prosecutor under Polish law;
2. the State from which the request for legal aid originates does not ensure reciprocity in this respect;
3. the request concerns an act which is not a crime under Polish law.

For situations which are not covered by the European Investigation Order, Art. 589l CCP constitutes the legal basis upon which a locally competent district court or public prosecutor shall execute without delay an order issued by a competent judicial authority of another Member State of the European Union, which may constitute evidence in the case of items, correspondence, consignments, lists of telephone connections or other transmissions of information or data stored in the IT system or on a carrier, including correspondence sent by email, if such items, correspondence, consignments, lists, data are located or stored on the territory of the Republic of Poland. The Polish law applies, but the authorities should also endeavour to satisfy the wishes of the requesting authorities concerning special procedures, if it is not contrary to the principles of the legal order (Art. 589r CCP).

2. Outgoing requests

Judges and prosecutors may issue requests for mutual assistance pursuant to Art. 585 CCP.

For situations which are not covered by the European Investigation Order, Art. 589g CCP provides that if it is established that items, correspondence, consignments, lists of telephone or other communications or data stored in an information system or on a carrier, including correspondence sent by email, are located on the territory of another Member State of the European Union, the court having jurisdiction to hear the case or the public prosecutor may apply for the execution of the order to detain or freeze them directly to the competent judicial authority of that Member State (§ 1). The competent court or prosecutor shall at the same time apply to the competent judicial authority of the executing State with a request for their transfer (§ 2). The European Judicial Network may be consulted in case of difficulties in determining the competent authority of the executing State.

3. Technical regulations

There are no rules on duties to filtering outgoing data or on the manner in which the transfer of the information should be carried out in the context of international cooperation. However, the Polish law applies as it is described above.

4. Real-time transfer of communication data

To the best knowledge of the authors there is no possibility for a foreign authority to access interception in real time being performed by the Polish authorities.

C. European Investigation Order

The European Investigation Order has been implemented by Poland by means of the law of 10 January 2018 that entered into force on 8 February 2018, which introduced chapters 62c and 62d CCP. The former deals with the rules where Poland is the requesting State, the latter where Poland receives requests.

In general the rules described in the previous parts of this chapter apply to requests regarding the control and recording of the content of telephone conversations and the recording by technical means of the content of other conversations or transmission of information, including correspondence sent by email (i.e., Arts. 237 ff. CCP).[125]

---

[125] Arts. 589w § 4 and 589ze § 10 CCP.

The only more specific rules regard the implementation of Art. 31 of the EIO Directive which is done in Art. 589zd (Poland as requesting State) and in Art. 589zt (Poland as a requested State).

D. Statistics

No statistics are available in this respect.

Bibliography

K. Boratyńska, Podsłuch komputerowy – zagadnienia wybrane. In: E.W. Pływaczewski (ed.), Aktualne problemy prawa karnego i kryminologii. Białystok 2005.

D. Drajewicz, Zakaz dowodowego wykorzystania procesowej kontroli rozmów. Państwo i Prawo 2011, No. 8.

K. Dudka, Kontrola korespondencji i podsłuch w polskim procesie karnym. Lublin 1998.

Z. Gostyński, R.A. Stefański, S. Zabłocki (eds.), Kodeks postępowania karnego. Komentarz. Warszawa 2004.

B. Grabowska-Moroz, Ochrona gromadzonych danych telekomunikacyjnych i zasady ich udostępniania na tle Konstytucji RP i prawa Unii Europejskiej – glosa do wyroku Trybunału Sprawiedliwości z 8.04.2014 r. w sprawach połączonych: C-293/12 i C-594/12 Digital Rights Ireland oraz do wyroku Trybunału Konstytucyjnego z 30.07.2014 r. (K 23/11). Europejski Przegląd Sądowy 2016, No. 1.

T. Grzegorczyk, Kodeks postępowania karnego. Komentarz. Warszawa 2008.

– Kodeksowe legalizowanie w procesie karnym, przez nowelizację z 11 marca 2016 r., dowodów uzyskanych za pomocą przestępstwa lub z naruszeniem przepisów postępowania albo poza granicami zgody udzielonej przez sąd na wkroczenie w sferę konstytucyjnie chronionych wolności jednostki. In: S. Steinborn, K. Woźniewski (eds.), Proces karny w dobie przemian. Zagadnienia ogólne. Gdańsk 2018.

W. Grzeszczyk, Kodeks postępowania karnego. Komentarz. Warszawa 2008.

P. Hofmański, E. Sadzik, K. Zgryzek, Kodeks postępowania karnego. Komentarz. Warszawa 2011.

B. Janusz-Pohl, Immunitety w polskim postępowaniu karnym. Warszawa 2009.

A. Kiedrowicz, Zagadnienie kontroli przekazów informacji w ramach telefonii internetowej. Prokuratura i Prawo 2008, No. 10.

R. Kmiecik, Kontrowersyjne unormowania w znowelizowanym kodeksie postępowania karnego. Prokuratura i Prawo 2015, No. 1-2.

P. Kosmaty, Podsłuch komputerowy. Zarys problematyki. Prokurator 2008, No. 4.

J. Kudła, A. Staszak, Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. Chmurze. Prokuratura i Prawo 2017, No. 7-8.

A. Lach, Dowody elektroniczne w procesie karnym. Toruń 2004.

– Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego. Prokuratura i Prawo 2013, No. 10.

– Przeszukanie na odległość systemu informatycznego. Prokuratura i Prawo 2011. No. 9.

G. Musialik, Dopuszczalność stosowania podsłuchu telekomunikacyjnego w stosunku do osób zobowiązanych do zachowania tajemnicy zawodowej na gruncie Kodeksu postępowania karnego z 1997 roku. Palestra 1998, No. 11-12.

L.K. Paprzycki (ed.), Kodeks postępowania karnego. Komentarz. Warszawa 2013.

K. Ponikwia, Uwagi krytyczne do Art. 239 k.p.k. Prokuratura i Prawo 2002, No. 10.

M. Rogalski (ed.), Prawo telekomunikacyjne. Komentarz. Warszawa 2010.

– Obowiązki przedsiębiorców telekomunikacyjnych na rzecz obronności i bezpieczeństwa państwa. Prokuratura i Prawo 2007, No. 12.

M. Rusinek, Tajemnica zawodowa i jej ochrona w polskim procesie karnym. Warszawa 2007.

M. Safjan, L. Bosek (eds.), Konstytucja RP. Komentarz, vol. I (Art. 1-86). Warszawa 2016.

A. Sakowicz (ed.), Kodeks postępowania karnego. Komentarz. Warszawa 2018.

B. Sitkiewicz, Wykorzystanie dowodów uzyskanych w ramach kontroli operacyjnej oraz podsłuchu procesowego. In: A. Lach (ed.), Postępowanie karne po nowelizacji z dnia 11 marca 2016 r. Warszawa 2017.

J. Skorupka, Krytycznie o stanowisku Sądu Najwyższego w kwestii legalności kontroli rozmów telefonicznych. Prokuratura i Prawo 2011, No. 4.

– Eliminowanie z procesu karnego dowodu zebranego w sposób sprzeczny z ustawą. Państwo i Prawo 2011, No. 3.

– Prokonstytucyjna wykładnia przepisów prawa dowodowego w procesie karnym. In: T. Grzegorczyk, R. Olszewski (eds.), Verba volant, scripta manent. Proces karny, prawo karne skarbowe i prawo wykroczeń po zmianach z lat 2015-2016. Księga pamiątkowa poświęcona Profesor Monice Zbrojewskiej. Warszawa 2017.

R.A. Stefański, Dowód nielegalny w postępowaniu karnym, in: S. Steinborn, K. Woźniewski (eds.), Proces karny w dobie przemian. Zagadnienia ogólne. Gdańsk 2018.

S. Steinborn, O zakresie ochrony immunitetowej w postępowaniu karnym. In: M. Kłopocka-Jasińska, M. Filipowska-Tuthill (eds.), Immunitet parlamentarny i immunitet głowy państwa z perspektywy konstytucyjnej i karnoprocesowej. Warszawa 2018.

K. Szczechowicz, Podsłuch telefoniczny w polskim procesie karnym. Olsztyn 2009.

D. Szumiło-Kulczycka, Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego. Warszawa 2012.

D. Świecki (ed.), Kodeks postępowania karnego. Komentarz. Warszawa 2018.

S. Waltoś, P. Hofmański, Proces karny. Zarys systemu. Warszawa 2018.

P. Wiliński, Konstytucyjny standard legalności dowodu w procesie karnym. In: S. Steinborn, K. Woźniewski (eds.), Proces karny w dobie przemian. Zagadnienia ogólne. Gdańsk 2018.

List of Abbreviations

bts	base transceiver station
CC	(Polish) Criminal Code
CCP	(Polish) Code of Criminal Procedure
dsl	digital subscriber line
IMEI	International Mobile Equipment Identity
IMSI	The International Mobile Subscriber Identity
ICT	Information and Communications Technology
IoT	Internet of Things
IP-traffic	Internet Protocol traffic
IT	Information Technology
MLA(T)	Mutual Legal Aassistance (Treaty)
MSISDN	Mobile Station International Subscriber Directory Number
MVNO	Mobile Virtual Network Operator
pos.	position
VoIP	Voice over Internet Protocol

Portugal*

National Rapporteur:
Pedro Verdelho

* This report outlines the legislation and case law as of May 2019.

Contents

I. Security Architecture and the Interception of Telecommunications

A. The General Architecture of the Legal System

1. In Portugal, as in several other countries, the legal framework recognises the interception of communications as an efficient procedural measure to obtain evidence in criminal investigations. Generally this investigative measure is only permitted in the context of criminal investigations, limited to serious cases and requires a judicial order.

2. Regarding penal proceedings, as a very general overview, in the Portuguese constitutional system, the criminal initiative lies with the Prosecution Service *(Ministério Público)*. All investigations are opened, directed and concluded by the order of a prosecutor who, according to the law, is assisted by the criminal police.[1] This constitutional model is explained in detail in the regular law. Article 2 of Law 49/2008,[2] of 27 August (Law on the Organization of the Criminal Investigation) states in paragraph 1 that "the direction of the investigation belongs to the judicial authority" who, according to paragraph 2, "shall be assisted by criminal police."

According to this system, during investigations, the role of the judge is related to safeguarding the fundamental rights of those under investigation.

Additionally, the Constitution of the Portuguese Republic, in Article 32, defines a number of specific safeguards related to criminal procedures, in line with the binding international instruments in force.

In particular, paragraph 8 of Article 32 states that "all evidence obtained by torture, coercion, infringement of personal physical or moral integrity, or improper intromission into personal life, the home, correspondence or telecommunications is null and void."

3. Currently, there are several public bodies who possess the status of *criminal police*. According to Law 49/2008, of 27 August (Law on the Organization of the Criminal Investigation) there are three generalist bodies of criminal police (which are *Polícia Judiciária*, *Guarda Nacional Republicana* and *Polícia de Segurança Pública*) and other (not listed) specific bodies of criminal police.

---

[1] As stated in Article 32 paragraph 5 of the Constitution of the Portuguese Republic, "criminal procedure possesses an accusatorial structure, and trial hearings and the committal-related acts that are required by law shall be subject to the adversarial principle."

[2] There is not an official translation of this law. A version, in Portuguese, can be found here http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1021&tabela=leis

B. Responsibility for the Technical Performance of Interception Measures

4. Historically, the execution of the investigative measures regarding interception of communications belonged to the *Polícia Judiciária*. In fact, since the first Internal Security Law (Law 20/87, of 12 June), confirmed by the second version of this Act (Law 53/2008, of 29 August), this police body has held the exclusive competence to intercept and control communications. This act (Law 53/2008, of 29 August[3]) expressly states, in Article 27, that "the execution of the control of communications is of the exclusive competence of the Polícia Judiciária."

Accordingly, resources have been allocated to the *Polícia Judiciária* to accomplish these tasks.

This does not mean that in concrete criminal investigations developed by other criminal police bodies (always under the direction of a prosecutor) the interception of communications is not permitted. On the contrary, the interception of communications can be done in investigations carried out by any criminal police body. However, in such cases these other bodies must seek the technical cooperation of the *Polícia Judicária* to make it operational.

In technical terms, in these cases, interception is effectively developed by the *Polícia Judicária*, which allows officers from other bodies to access its technical premises, to follow on and obtain the output of the interception.

Article 27 section n)[4] of Law 5/2004, of 10 February (Law Applicable to Electronic Communications[5]), states that providers of publicly available electronic communications networks and services shall make available, at their own cost, "systems of legal interception to competent national authorities, as well as the supply of means of decryption or decoding where these facilities are present."

---

[3] A Portuguese version of this act is available at http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1012&tabela=leis

[4] Article 27 General conditions

1 Without prejudice to other conditions provided for in general law, undertakings providing publicly available electronic communications networks and services may be subject in the exercise of their activity to the following conditions:

(…)

n) Installation, at the undertaking's own expense, and provision of systems of legal interception to competent national authorities, as well as the supply of means of decryption or decoding where these facilities are present, in accordance with legislation governing personal data and privacy protection within the scope of electronic communications;

(…)

[5] Law 5/2004 of 10 February transposed to the Portuguese legal framework Directives 2002/19/EC, 2002/20/EC, 2002/21/EC and 2002/22/EC, all of them of European Parliament and of the Council of 7 March 2002, and also Directive 2002/77/EC of the Council of 16 September. An English version of this act is available at https://www.anacom.pt/render.jsp?contentId=975162

Thus, providers are responsible for installing a technical system that allows law enforcement authorities to intercept communications. Moreover, if the communications they provide are encrypted, they shall make available means of decryption. Obviously, this obligation does not cover services by other providers, which may be transmitted through its network.

C. Statistics on Electronic Communication Interception

5. In Portugal, statistics regarding interception of communications are not publicly available. As will be explained in more detail, this type of procedural measure requires (among other things) authorisation from a judge. This judge may be any judge, in any *comarca* (district) of the country, depending on its territorial and substantive position: if there is need to request authorization to implement interception of communications in a particular case, the prosecutor will address the judge in the local criminal court.

In other words, there is no central authority in charge of issuing such orders which, in any case, may be potentially requested within criminal investigations dealt with by any prosecutor, in each one of the investigation departments of the *Ministério Público*.

There is also no legal obligation to keep statistical records of such investigative measures – nor is there for the majority of procedural measures.[6] The measure is based on and decided for a particular investigation and the only record that will be kept is for the purposes of that particular investigation.

Certainly the *Polícia Judiciária* keeps records and files of all judicial orders regarding the interception of communications, because it is a specific competence of this police body to ensure all such technical acts. But these records do not provide a rigorous picture or precise figures of the phenomenon, as it is frequently the case that judicial orders cover more than one telephone number or more than one device.

6. Regarding international cooperation, the question is even more diffuse, as no statistical records are kept regarding the scope of the requests. Both when acting as requesting State and requested State, no record of the nature and purpose of the requests is kept, which are filed by requesting and requested State.

Moreover, in the current European and national legal framework,[7] it may be very difficult, if not impossible, to obtain accurate figures at this respect as, at least in theory, it is possible to request interception of communications, from one country

---

[6] Thus, there is also no statistical record of, for example, searches or of seizures of objects.

[7] Namely under the European Investigation Order.

to another country, directly, from one judicial authority to another judicial authority, without the intervention of a central authority.[8]

II. Principles of Telecommunication Interception in Constitutional and Criminal Procedural Law

A. The Constitutional General Approach

7. As stated before, it is assumed in the Portuguese constitutional and legal system, that the interception of communications may be used in the course of criminal investigations. But on the other hand, it is also recognised that such a measure may interfere seriously with the fundamental rights of citizens, namely privacy, private and family life, and secrecy of communications. Thus, the constitutional text, itself, even if adopting a tolerant view in this respect, on the other hand also imposes serious thresholds to the use of interception of communications.

Accordingly, the penal procedural law introduces a control process, requiring the mandatory intervention of a judge. As mentioned above, according to the Portuguese system, the *owner* of the investigation, that is, the authority to whom the competence to direct the investigating phases was legally attributed, is a prosecutor and the intervention of a judge is required only as the *guardian of the safeguards* of the citizen.

B. Constitutional and Legal Principles Regarding Interception of Communications

8. At this point, it is important to note that secrecy of communications is, within the Portuguese constitutional system, a constitutionally recognised right, described in the articles of the fundamental text. In fact, Article 34 paragraph 1[9] Constitution[10] states that "private communications are inviolable," as well as "secrecy of correspondence." Moreover, Article 34 paragraph 4 states that "public authorities are prohibited from interfering in any way with correspondence, telecommunications or other means of communication." Of course, an exception is foreseen and related to "the cases in which the law so provides in matters related to criminal procedure."

---

[8] Article 3 of the Directive 2014/41/EU, from the European Parliament and of the Council, from 3 April 2014, that defines the European Investigation Order, states that this type of measure may be used with respect to all the investigative measures, except to create a JIT.

[9] See Appendix.

[10] An official translation into English of the Constitution of the Portuguese Republic may be found here https://dre.pt/constitution-of-the-portuguese-republic

Thus, the constitutional framework is rather clear, prohibiting, in general, the interference of all public authorities in telecommunications, with the sole exception of concrete situations of legal criminal procedures.

9. Two important observations can be made here. The first one concerns the wording and concepts enshrined in Article 34 Constitution. The text refers to "telecommunications or other means of communication." Internet, email, mobile communications, and other types of digital or electronic communications are not expressly mentioned in the constitutional text.

One must recall that this text was first drafted in 1976 (even if amended in 1997), more than 40 years ago when much of this new technology only existed in the fertile minds of science fiction writers. On the other hand, the spirit of the provision is to keep all human communications confidential through any technical means – clearly intended by the last part of the sentence, which reads "other means of communications." Accordingly, a proper reading and interpretation of this article should extend the protection to all types of private communications between two people who are not in the presence of one another, using technological means.

10. The second remark regards the exception to this general rule and its respective scope. The constitutional text is also clear on this: interfering in telecommunications or other means of communication is solely allowed "in the cases in which the law so provides in matters related to criminal procedure." The constitutional text does not specify the particular cases where interception of communications is allowed, leaving it to the regular law. However, this limits the possibility to the specific cases typified in the law.

On the other hand, however, the Constitution does not leave all the possibilities to the regular law. On the contrary, it expressly limits the legal possibility of intercepting communications to criminal procedure.

This is a very important conclusion as, departing from it, it becomes very clear that intercepting communications is not allowed in any other intervention of the public authorities, other than in the context of a criminal investigation, under the framework of the Code of Penal Procedure. For example, intervention in communications is not allowed in the context of national security activities, or within the activities of the intelligence or information services.

11. These provisions of the Constitution of the Portuguese Republic cannot be read in isolation and are complemented by Article 18. In particular, they need to be understood in consideration, particularly, with paragraphs 2 and 3 of Article 18, which clearly call for proportionality in any restriction, by the legal rules, to the fundamental rights described and enshrined in the Constitution.[11]

---

[11] See Appendix.

In fact, paragraph 2 provides guidance to the legislator in this respect, stating that "the law may only restrict rights, freedoms, and guarantees in cases expressly provided for in the Constitution, and such restrictions must be limited to those needed to safeguard other constitutionally protected rights and interests."

On the other hand, paragraph 3 obliges the legislator to intervene having in mind that "laws that restrict rights, freedoms, and guarantees (…) may not (…) reduce the extent or scope of the essential content of the constitutional precept."

In this case, proportionality means that the legislator needs to consider principles such as adequacy, proportionality *stricto sensu*, and necessity. Adequacy may be met by ensuring that the means used are suitable for the purpose. Proportionality *stricto sensu* requires a careful analysis of the particular case, in view of finding a balance between the means used and the purpose of the action. Finally, necessity highlights the need to consider other alternative means before adopting such a measure.

12. In conclusion, according to the Constitution, even if the measure is allowed, it is also recognised that intercepting communications violates the constitutional rights of the individual, such as private or family life – as stated in Article 26 Constitution.[12] Thus, according to the constitutional framework, the law only allows the interception of communications within very strict limits.

First of all, one should keep in mind that the use of this investigative tool is limited to a legal criminal investigation. Additionally, according to the Constitution this measure can only be authorised related to certain types of crime. The criterion of proportionality requires the legislator to further filter the measure and to allow it only in certain cases, for example, where more serious crimes are investigated, or in cases where no other measures would be effective.

13. However, in this respect, the Constitution of the Portuguese Republic goes further, protecting citizens against abuse by public authorities. In fact, despite not providing concrete guidance around the implementation of the intercept of communications, Article 32[13] Constitution contains a very important provision in paragraph 8. It states that "all evidence obtained by torture, coercion, infringement of personal physical or moral integrity, or improper intromission into personal life, the home, correspondence or telecommunications is null and void."[14]

14. The prohibition on interference by public authorities in telecommunications is expressly provided in the substantive penal ordinary law: the Penal Code punishes, in Article 384, the breach of telecommunications secrecy. This rule provides for

---

[12] See Appendix.

[13] See Appendix.

[14] As it will be more specified in another section, this provision has concrete consequences in criminal proceedings, as stated in Article 126 Code of Penal Procedure.

the punishment of "postal, telegraphic, telephone or telecommunications services officer who, without being duly authorized, discloses to third parties communications between certain people by mail, telegraph, telephone or other means of telecommunications of those services, of which he was aware because of his duties." The provision also incriminates the officer who "records or discloses to third parties the content (…) of the communications referred to."

15. This type of crime appears anachronistic in its wording. It was evidently drafted in the past, when long distance communication required the active intervention of technical operators. In the modern world of digital communications, the ability of the operator's employees to interfere with actual communications has dramatically reduced the real possibility of verifying this type of crime.

To this technical obstacle to the verification of this crime presented by modern day communications, can be added another obstacle, of equal measure, which renders the verification of this type of crime practically impossible, making it a very rare crime. It was created at a time when telecommunications services were companies owned by the State, or even part of the Public Administration, and the crime in question could be committed by telecommunications service officials only. Article 386 Penal Code defined employees for these criminal purposes, and did not include employees of private entities.

Nowadays, however, electronic communications are liberalised and the activity can be carried out by anyone, as a result of Article 19 paragraph 1 of Law 5/2004, of 10 February (Electronic Communications Law). In current law, telecommunications services are therefore not public services but private. As noted, the crime foreseen in Article 384 Penal Code is not currently applicable to private operators and is therefore only potentially applicable – if they still exist – to managers, owners of supervisory bodies, and workers of public companies, nationalised, of public capital or with a majority share of public capital.

16. Nevertheless, Article 384 Penal Code does not exhaust the range of crimes in this area. In fact, the crimes contained in Articles 194 and 195 Penal Code actually may be committed by any person. Article 194 provides, under the heading "breach of correspondence or telecommunications," that those who, without consent, "interfere in the content of telecommunications or become aware of it" will be punished – paragraph 2. Those who merely disclose the content of telecommunications can also be punished.

If in a particular case the typical elements of Article 194 are not present, it is possible that Article 195 might apply. The latter is a residual crime, punishing the unlawful disclosure of any secrecy which the agent has learned by virtue of his capacity, job or profession.

17. Another example of the protection of secrecy of communications in the Substantive Penal Law can be found in Article 276 Penal Code, which punishes the mere detention of equipment intended for breach of telecommunications.

In practice, this article incriminates those who possess devices, or any type of technical equipment specifically intended for telephone wiretapping or violation of telecommunications, without fulfilling the legal conditions. The latter are specified in the penal procedure rules (namely in Articles 187, 188 and 189 Code of Penal Procedure and in Article 18 Law on Cybercrime (Law 109/2009, of 15 September[15]).

18. A legal reference to telecommunications secrecy can also be found in Law 41/2004 (protection of personal data and privacy in electronic communications).

This act fully recognises and implements the constitutional principle of the inviolability of telecommunications. Article 4 paragraph 1 Law 41/2004 states that service providers shall preserve the inviolability of communications and traffic data. Article 4 paragraph 2 prohibits the interception and monitoring of communications.

Therefore, this law, embracing the constitutional matrix, draws up the protection of the confidentiality of communications on two levels: on the one hand, it requires service providers to ensure the inviolability of such communications and traffic data; and on the other hand, prohibits interception, interception devices, storage or surveillance of communications, and traffic data by third parties without the express prior consent of the users.

19. Law 41/2004 was enacted with the purpose to implement, at the national level, the European Directive 2002/58/EC[16] of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).

It originally provided very restrictive solutions, imposing an obligation on service providers to supress traffic data as soon as it is unnecessary – in particular after billing and payment by customers. This is set out in Article 6 paragraph 1, which states that traffic data relating to subscribers and users shall be deleted or made anonymous when it is no longer necessary for the purpose of transmitting the communication. Paragraph 2 provides an exception for the processing of traffic data necessary for subscriber billing and interconnection payments, but this treatment is only allowed until the end of the period during which the invoice can be legally disputed, or the payment claimed.

---

[15] An English version of the Law on Cybercrime is available at http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/portuguesecybercrime_law.pdf

[16] Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

Nevertheless, in practice, this provision must be read (and it is, by practitioners) in a different manner. The issue will be explored in another section.

C. Other Constitutional Principles Regarding Information Technology

20. In the Portuguese constitutional and legal system, data protection rules are fully in line with the European standards.

Within the constitutional framework data protection itself is not expressly considered – which is normal, in a text drafted primarily in 1976, even if revised and amended a number of times (the last amendment to the Constitution, the seventh revision, was approved in 2005). However, Article 35 Constitution describes the so-called fundamental rights related to the *use of information technology*[17] and, in practice, enshrines, as a fundamental right, most of the main principles also considered in the relevant international instruments.

In paragraph 1, Article 35 defines the right of the citizen to *access computerised data* that concerns him, and to correct and update the data, as well as the right to be informed of the purpose for which it is intended. Paragraph 3 introduces limits to using of "information technology (…) to treat data concerning philosophical or political convictions, party or trade union affiliations, religious faith, private life or ethnic origins."

III. Authority to Access Telecommunication Data in the Law of Criminal Procedure

A. Background

1. The Code of Penal Procedure and other acts

21. Since 1987, the Code of Penal Procedure has provided for rules relating to interception of telephone communications – namely in Articles 187 to 190.

Article 18 Law on Cybercrime[18] (Law 109/2009, of 15 September) adapted the legal system of interception of communications to *digital crimes*, provided for in the Code of Penal Procedure.

---

[17] See Appendix.

[18] See Appendix.

22. A preliminary question regarding the compatibility of both legal frameworks must be asked, namely in view of Article 189,[19] which extends the applicability of Articles 187 and 188 to "communication transmitted through any technical means."

In fact, even before the Law on Cybercrime was passed, the Code of Penal Procedure already covered the interception of electronic communications – and not only telephonic communications, as foreseen in Article 187. However, this extension did not apply to investigations regarding computer or computer-related offences, because the scope of this particular framework, by the means of this extension, was exactly the same as for telephone interceptions. In this context, for example, none of the crimes described in the Law on Cybercrime were included in the closed number of crimes listed in the catalogue of Article 187 Code of Penal Procedure.

The Law on Cybercrime, through its Article 18, did adapt to the digital environment the system of interception of communications provided for in the Code of Penal Procedure. However, this general regime of interceptions was not expressly repealed by the Law on Cybercrime, the purpose of which was to set up a special procedure designed to be applied in specific cases, as provided for in its Article 11.[20]

Thus, the purpose of Article 18 Law on Cybercrime was precisely to extend interception of communications to a number of additional types of crimes – those described under that act. The rest of the law merely transposes the mechanism of interception of communication provided for in the Code of Penal Procedure into the digital environment. In fact, it seems that it deliberately refers to the general regime and, therefore, assumes that the interception of communications provided for in the law shall follow Articles 187 and 188 Code of Penal Procedure. In fact, there is an express reference to those provisions in Article 18 paragraph 4 Law on Cybercrime but, further than that, the criteria permitting the interception of communications under this act (according to Article 18 paragraph 2 Law on Cybercrime) are exactly the same as provided for in Article 187 Code of Penal Procedure. In fact, Article 18 just goes further in defining the material scope to which it applies. As has been previously noted, most of the crimes defined under this law (which are *computer crimes*, or *cybercrimes*) are not included in the catalogue provided for in Article 187 and, therefore, the interception of communications is not allowed when investigating these crimes.

In conclusion, this special regime did not repeal or interfere with the regime provided for in Article 189 Code of Criminal Procedure, though it did create a special regime, with a limited scope.[21] Article 189 remains in force for all other cases.

---

[19] See Appendix.

[20] See Appendix.

[21] This was also decided by the rulings of the Évora Court of Appeal *(Tribunal da Relação de Évora)* of 6 January 2015 (available in Portuguese at http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?Open

23. The provisions of Article 18 Law on Cybercrime meet the requirements of Articles 20 and 21 of the Council of Europe Convention on Cybercrime, also known as the Budapest Convention, which provides for rules related to the real-time collection of traffic data and the interception of communications.

2. Data in possession of the providers

24. The Portuguese legal framework recognises that nowadays, in criminal investigations, it is increasingly necessary to obtain information from service providers – above all, regarding the identification of who established a particular communication. Service providers keep information regarding the identification of their customers (name, address, etc., also known as subscriber information) and concerning the communications established by them – so-called traffic data.

Providers do not keep – since it is forbidden to do so – the content of communications. According to the Portuguese law, obtaining the content of communications is only possible through the interception of communications, in real time, under the terms of Articles 187 and 188 Code of Criminal Procedure and Article 18 Law on Cybercrime. Of course, this is only valid with regard to future communications.

25. There are multiple legal acts which simultaneously govern the obtaining of data held by service providers in criminal proceedings: the Code of Penal Procedure (namely Article 189 paragraph 2), Law 32/2008, of 17 July and, finally, the Law on Cybercrime (Law 109/2009, of 15 September). However, their wording is not always compatible, which creates uncertainty in the application of the law to a particular case, with consequent doubts as to the validity of the obtained evidence.

Article 189 Code of Penal Procedure (which was introduced by the amendment of 2007 – Law 48/2007, of 29 August) regulates the obtaining, *inter alia*, of "records of established communications." It determines that this evidentiary proceeding follows the procedural regime of interceptions of telephone communications (as already mentioned, described also in Articles 187 and 188 Code of Penal Procedure).

Moreover, Law 32/2008[22] regulates traffic data retention. It creates an obligation, for all the providers of communications, to retain their customers' data (including traffic data) for a period of one year. This act introduced a special procedural regime for accessing such data, which makes access to it subject to a "reasoned order of the investigating judge, if there is reason to believe that diligence is indispensable for the discovery of the truth or the evidence would otherwise be impossible or

---

Document) and of 20 January 2015 (available, in Portuguese, at http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument).

[22] There is no translation of the law. A Portuguese version is available at https://dre.pt/application/dir/pdf1sdip/2008/07/13700/0445404458.PDF

very difficult to obtain in the investigation, detection, and prosecution of serious crimes" – Article 9 paragraph 1.

Unfortunately, the conciliation of these three regimes was not intended by the legislator, thus requiring an additional effort from the interpreter. Only the necessary coexistence of Law 32/2008 and the Law on Cybercrime was referred to. Indeed, in Article 11 paragraph 2 Law on Cybercrime, it is determined that what is stipulated in it does not affect the regime of Law 32/2008.

3. Traffic data

26. As mentioned above, by applying the general rules of succession of laws in time, it must be concluded that Article 189 Code of Penal Procedure has been partially repealed by the Law on Cybercrime. Despite this, the section referring to records of communications, mentioned in Article 189 paragraph 2, remains in force. In fact, it has never been expressly repealed. However, no other provision, particularly in the Law on Cybercrime, replicates it, and consequently it remains in force to regulate the collection of traffic data or, in the telephone context, billing information. It is therefore in accordance with this regime that all requests from the prosecutor to providers must be processed.

It should be noted that this legal regulation does not prevent obtaining information stored in devices, for example, in the context of a search of a mobile telephone (or a laptop or other device). The data referred to in Article 189 paragraph 2 Code of Penal Procedure concerns only records stored by the service providers and not the records stored by the device itself. This is because the constitutional and legal protection of telecommunications secrecy affects only the relationship of trust established between the operator and the customer and does not exist when, in a legitimate manner, the investigation has access to the individual's device. These cases, where, through legitimate access to a mobile phone or other device, access to records of communications is granted, are governed by Article 17 Law on Cybercrime.

4. Subscriber information

27. 'Subscriber information' as it is known internationally, now referred to in Article 14 Law on Cybercrime, was traditionally known as 'basic data' in Portuguese doctrine and jurisprudence. This includes information "in possession of the providers, relating to their customers or subscribers, including any information other than traffic or content data." This data set includes information about the IP address used in a particular communication.

Within an investigation, it is the responsibility of the public prosecutor to request information from service providers relating to the identity of their customers – for example, information referring to a particular user that in a given time context

(day and time) used a specific IP address. The same reasoning is applicable to the situation where the investigation needs to know the specific IP address used by a given customer of a provider. Thus, although this type of information may technically be classified as traffic data, according to Article 14 paragraph 4 letter b Law on Cybercrime, the legal regime for obtaining is the same as that of the so-called basic data, or subscriber information.

It should be noted that the data in question will have to be "computer data or in any other form held by the service provider." This procedural measure therefore should not be confused with the preservation of data nor with the expedited disclosure of preserved data – preservation is proactive and aims at the conservation of data that would not otherwise be preserved. On the other hand, this legal formula means that providers are only obliged to supply the data that they actually store.

5. Data retention period

28. As regards traffic data, there are two different and complex legal regimes obliging data providers to store data: the first – the general regime – is provided for in the Law on Cybercrime, the Law 41/2004 and Article 189 paragraph 2 Code of Penal Procedure; the second – the special regime – is provided for in Law 32/2008.

29. Under the general regime (meaning, outside the context of Law 32/2008), no specific term for traffic data storage is provided for. However, as a whole, the regulatory framework allows operators to retain such data for six months. Therefore, unless one of the specific crimes referred to in Law 32/2008 is involved, the period for which operators can retain traffic data is six months, and consequently, this is also the period during which they have the obligation to provide this data to the criminal authorities, within an investigation. The reason for the six-month period is explained below.

Article 4 paragraph 2 of Law 41/2004 stipulates a general prohibition on the storage of traffic data, safeguarding only the exceptions determined by the law itself. This prohibition is corroborated by Article 6 paragraph 1 of the Law, which stipulates that "without prejudice to the provisions of the following paragraphs, traffic data relating to subscribers and users processed and stored by undertakings providing electronic communications networks and/or services shall be deleted or made anonymous when they are no longer necessary for the purpose of the transmission of the communication." That is, the legal framework in force provides, as a general principle, the obligation to delete traffic data as soon as the communication ends. It should be stressed that this provision is not in conflict with Law 32/2008, which is more recent and has clearly introduced additional exceptions to this prohibition.

30. However, the same Article 6 of Law 41/2004, in paragraphs 2 and 3, introduces exceptions to this prohibition in paragraph 1, stipulating that the traffic data

which is necessary for billing purposes may be stored and processed until the end of the period during which the invoice can be legally claimed in court.

This act (Law 41/2004) does not establish the legal term for claiming invoices. However, Law 23/96, of 26 July, establishes rules regarding the provision, by companies, of essential public services (electricity, water, telephone, etc.), and stipulates, in its Article 10 paragraph 1, that "the right to receive the price of the service provided is limited to six months after its provision." This statement is corroborated by Article 10 paragraph 4, which also sets a six-month time limit for the claim by the service provider. The regime defined in this legal act is applicable to electronic communications services, in view of Article 1 paragraph 2 letter d of the same act.

In short, with regard to the provision of electronic communications services, the period of time that a service provider has to claim the due payment of its invoice is six months – consequently, the provider may store the required information for six months. Once these six months have elapsed, the obligation to eliminate traffic data, established by Article 6 paragraph 1 of Law 41/2004, must be effectively applied. It is only then that the generic prohibition on traffic data retention, enshrined in Article 4 paragraph 2 of the same law, becomes effective. Therefore after six months, the traffic data generated by a particular communication must be eliminated and can no longer be legally held by service providers.

31. Among the data that the judicial authority is entitled to request, based on Article 14 paragraph 4 Law on Cybercrime, is, as mentioned, the identification and location data of its customers – traditionally known as "basic data." The law does not impose any period of custody or disposal relevant to such data.

Article 14 paragraph 4 Law on Cybercrime is also the usual grounds to justify obtaining, in investigations, the identity of the user of an IP address used by a particular customer of a provider, as long as it is related to a concrete investigation. However, since the IP address falls within the technical category of *traffic information*, operators can only keep it for six months. Therefore, judicial authorities are entitled only to request data relating to communications which have occurred within the six months preceding the request, since only such data can be legitimately held by the service provider.

6. The validity of the data retention law

32. As already mentioned, the Portuguese legal framework includes a data retention system, established by Law 32/2008, of 17 July 2008, which transposes into the domestic legislation the Directive 2006/24 of the European Parliament and of the Council, of 15 March.

This domestic legal act, in compliance with the obligation to transpose that Directive, obliges service providers to retain data (in particular traffic data). However,

the ruling of the European Court of Justice (of the European Union) of 8 April 2014 in the *Digital Rights Ireland*[23] case, declared the Data Retention Directive invalid.

33. The need for the retention of data relating to electronic communications is broadly accepted as a very important auxiliary tool within criminal investigations. The absence of data retention in those countries where it has no legal recognition, has deprived the criminal and judicial authorities of an important source of information and evidence. It is also assumed that such retention of data should be *prima facie* circumscribed to criminal investigation procedures within criminal justice – it is not universally accepted that it is usable for national security or intelligence purposes.

Since the retention of traffic data is essential, the important discussion is not its admissibility, but rather the conditions under which it takes place: security measures and legal safeguards regarding storage, custody, access, and destruction of data after the retention period. Also important are the control of its use (judicial, in particular) and limiting the use, for example, to investigations of more serious crimes.

The wording of the judgment of the European Court of Justice of 8 April 2014 is explicit in this regard, namely underlining the need for regulating data retention.

Following this ruling several European countries by the means of parliamentary decisions or rulings of constitutional courts, have declared their national laws transposing the Data Retention Directive invalid. Portugal, however, considers that this national act is still in force.

34. Indeed, from the legislative point of view, the need to introduce a change was not felt – no legislative initiative has been tabled.

The jurisprudence on the practical application of Law 32/2008 is not very extensive and focuses mainly on other aspects – not on the impact of the judgment of 8 April on the Portuguese law.

However, a recent decision by the Constitutional Court, of 13 July 2017,[24] focused on the validity of the law in the face of the European jurisprudence.[25] In short, the Constitutional Court stated that the obligation imposed on providers to

---

[23] *Digital Rights Ireland Ltd* (C 293/12) against *Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána and Irish Human Rights Commission*; and *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* (C 594/12).

[24] The full text of the ruling, even if in Portuguese only, is available at http://www.tribunalconstitucional.pt/tc/acordaos/20170420.html

[25] In addition to the *Digital Rights Ireland* case, this ruling of the Portuguese Constitutional Court also took into account the doctrine of the more recent *Tele2 Sverige* case (C-203/15), a ruling by the European Court of Justice of 21 December 2016 (http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203&lang1=pt&lang2=EN&type=TXT&ancre=).

retain data in the framework of Law 32/2008 is not against the Portuguese Constitution, despite the ruling invalidating the European Directive which framed the national law.

This ruling reflects a general understanding, shared by the judicial community and telecommunication providers, to the effect that Law 32/2008 is still in force.

It is important to underline that Law 32/2008, in addition to the formal transposition of the full text of Directive 2006/24/EC, also introduced a much more complex framework regulating the data retention process. For example, it fixed rules regarding who is authorised to access the data or the conditions of storage and access to the data. In fact, the national law went well beyond the requirements of the Directive and most of the requirements specified in the ruling of the European Court of Justice had already previously been considered in the domestic law. For that reason, it was held that the European Court's ruling does not affect the validity of the national law.

As an example, Portuguese law stipulates conditions for the access to data, requiring disclosure to be preceded by a judge's order (as stated in Article 9 paragraph 1 of Law 32/2008). This condition, unlike the Directive, provides for the requirement of authorisation by an independent authority in accessing the data, and would, therefore, not attract the same criticism as the Directive in the European Court of Justice.

Furthermore, the Court considered that the Directive did not provide for the obligation to delete the data after the retention period. The Portuguese law establishes the exact opposite, imposing the destruction of the data after the retention period (as stated in Article 7 paragraph 1 letter e Law 32/2008).

With regard to data retention, the European Court of Justice also underlined the lack of regulatory requirements with respect to the retention process. Once again, the Portuguese law provides for rules that impose important safeguards in this regard (for example, who is authorised to access data, strict storage conditions, and others).

7. The constitutional background regarding criminal investigations

35. In the Portuguese penal procedure system, constitutional rules may apply directly, if required, in order to safeguard fundamental rights. That is, the Constitution applies directly, over the ordinary law, when a constitutional right is challenged by any investigative activity or measure. This is an important standard, as the constitutional text itself provides a list of rights and principles related to criminal investigation.

Article 32 Constitution,[26] along with international instruments in this respect, defines several safeguards that must be observed by all criminal procedures. Some general principles are enshrined in this provision, such as the right to appeal (in paragraph 1), or the presumption of innocence (in paragraph 2), or the right to choose a defence lawyer and to be assisted by him in relation to every procedural act (in paragraph 3).

Following this spirit, the Penal Code[27] also establishes fundamental rights and principles, such as the principle of legality (mainly in the facet of *nulla poena sine lege*), enshrined in Article 1[28] paragraph 1.

At the same level of fundamental rights, Article 1 paragraph 3 defines another very important general rule that all criminal investigations must observe: the absolute prohibition on using analogy to qualify an act as a criminal offence, or to determine a criminal penalty.

36. In the field of procedural rules some fundamental rights are mentioned at the level of ordinary law. For example, Article 126[29] Code of Penal Procedure describes several circumstances where obtaining evidence is not valid.

Article 126 paragraphs 1 and 2 contain the prohibition on obtaining evidence through torture, coercion or, in general, through offence to the physical or moral integrity of people. According to these rules, all evidence obtained with infringement of this prohibition "shall be null and void and may not be used."

Relevant to the subject of this report, Article 126 paragraph 3 Code of Penal Procedure prohibits obtaining evidence "through intrusion in private life, at home, in correspondence or in telecommunications except for cases provided for by law," or with the consent of the holder of the right. In case of infringement of this prohibition, the evidence obtained is also null and void.

This mechanism reinforces that all criminal investigations must respect the fundamental rights: if evidence is illegally obtained, with a violation of fundamental rights, that evidence will not be able to be produced and will be devoid of value.

---

[26] See Appendix.

[27] The English version of the general part of the Portuguese Penal Code is available at http://www.verbojuridico.net/download/portuguesepenalcode.pdf

[28] Article 1 Principle of legality

1 An act may only be criminally punished if it was determined punishable by law before the act was committed.

2 Security measures may only be applied to cases of perilousness, if its conditions are determined by law previous to its fulfilment.

3 An appeal to analogy is not permitted to qualify an act as criminal, to define a case of perilousness, or to determine a penalty or a corresponding security measure.

[29] See Appendix.

Moreover, Article 126 paragraph 4 Code of Penal Procedure goes further and states that if "methods of obtaining evidence that constitute a crime" are applied, the obtained evidence may only be used for the exclusive purpose of proceeding against the agents of that crime.

B. Interception of Content Data

37. The general framework of interception of telephonic communications is described in Articles 187 to 190 Code of Penal Procedure.[30] Article 187 describes the admissibility and conditions, Article 188 refers to the formalities of the operations, and Article 189 extends the rules of telephonic interception to other types of electronic communications and to obtaining records of communications. Finally, Article 190 states simply that the "requirements and conditions referred to in Articles 187, 188 and 189" must be observed "under penalty of nullity."

1. General overview

38. As stated before, by constitutional imposition, interception of communications is solely allowed in the cases provided for in the law. Article 187[31] Code of Penal Procedure is the main reference in this respect.

This provision defines the general conditions according which an interception of communications can be authorised. It also lists the types of crimes the investigation of which can involve an interception of communications. Article 187 defines the admissible targets of interception of communications. Finally, some procedural rules are also stated, both in Article 187 and Article 188.

As has already been noted, the authorisation to perform interception of communications within a criminal investigation shall be issued by a judge, and must be justified. In any case, this measure will always be a result of an initiative from a prosecutor (as a consequence of the accusatorial system, where the criminal initiative belongs to the Prosecution Service).

2. Interception as ultima ratio

39. Even if interception of communications is recognised as an important tool when investigating crimes, the Portuguese system sees this procedural measure as a last resort, reserved for situations when other possibilities are not available or will not be efficient. In fact, this means of obtaining evidence can only be authorised by

---

[30] An unofficial English version of the Code of Penal Procedure, which was used in this text, is available at http://gddc.ministeriopublico.pt/sites/default/files/documentos/pdf/code_of_criminal_procedure_english.pdf

[31] See Appendix.

a judge and "may only be authorised during the inquiry where there are grounds for believing that this step is indispensable for the discovery of the truth or that the evidence would, by any other means, be impossible or very hard to collect."

It is clear that, for example, the mere possibility that an interception could contribute to the "discovery of the truth" is not enough to justify an order of interception. The emphasis is on the expression "indispensable for the discovery of truth," which recalls the constitutional principle of necessity.

Thus, interceptions of communications should only occur after other possible available means have been exhausted, or when other possibilities (in a prognosis judgment) are believed not to be effective, or for any reason, are excluded. Accordingly, interception of communications can never be used because it may be the fastest or the easiest or even the most effective means to investigate.[32]

3. Interception in the context of a criminal investigation

40. It seems obvious, and has already been mentioned, but it must be underlined again that, within the Portuguese system, the interception of communications may only be authorised in the context of a criminal investigation. Thus, it is not possible to perform an interception as a preventive measure, or just for the purposes of gathering intelligence. As stated before, this a constitutional requirement (Article 34 paragraph 4 Constitution).

It is also the case that a judge, by his own initiative, cannot decide to authorise an interception: he is limited by the initiative of a prosecutor. Both the request of the prosecutor and the decision of the judge on interception must be based on concrete motivations which are stated in the request and decision.

Besides the general constitutional principle of the obligation to substantiate grounds for all judicial decisions, enshrined in Article 205[33] Constitution, in this case, the requirement goes even further, as interception of communications is seen, in the system, as an investigative resource of *ultima ratio*.

---

[32] However, interestingly, according to the jurisprudence, this principle legitimates, for example, the use of interception of communications as the first investigative measure in the investigation, if it is believed that it will be the only possibility of bringing to the investigation evidentiary elements capable of discovering the truth. This is the case of the ruling of *Tribunal da Relação de Évora* of 5 May 2015 (available, in Portuguese only, at http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/f3f7d3bde2479bad80257e4a003a277b?OpenDocument) and of the ruling of *Tribunal da Relação de Évora* of 17 March 2015 (available, in Portuguese only, at http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/6a827b6477ada98880257e20003c4c74?OpenDocument).

[33] See Appendix.

4. Types of crimes

41. One of the most important restrictions to interceptions of communications is the so-called catalogue of crimes described in Article 187 paragraph 2 Code of Penal Procedure. According to this provision, interception of communications may only be authorised in the context of an investigation of a limited number of crimes.[34] This is clearly a result of the desire for interception of communications to be exceptional, motivating the legislator to limit its use to a closed list of possibilities. Article 34 paragraph 4 Constitution also limits interception of communication to "cases provided for by law in criminal matters."

It is not evident what criteria the legislator followed in order to define this list of crimes. One can say that the general threshold is established in Article 187 letter a Code of Penal Procedure, that limits interception of communications to "criminal offences to which a custodial sentence with a maximum limit over three years applies." This provision defines a minimum standard of "seriousness," thus following the constitutional principle.

However, it is not clear why some of the other included offences were listed.

5. Targets

42. Another important constraint on implementing the interception of communications is the personal factor. According to the Portuguese law, the possible targets of an interception are limited and also listed. According to Article 187 paragraph 4 Code of Penal Procedure, an interception only may have a concrete and identified target.

This particular provision limits the possibilities of interception to the suspect or defendant, or to any person acting as an intermediary (someone against whom there are grounds to believe receives or transmits messages aimed at, or coming from, the suspect or defendant) or, finally, a victim of a crime (but on this case, only upon his effective or alleged consent).

---

[34] The following criminal offences:

a) Criminal offences to which a custodial sentence with a maximum limit over three years applies;

b) Illegal restraint, kidnapping and taking of hostages;

c) Offences against cultural identity and personal integrity, as provided for in Book II, Title III, of the Criminal Code and in the Criminal Law on Violations of International Humanitarian Law;

d) Offences against State security foreseen in Book II, Title V, Chapter I, of the Criminal Code;

e) Counterfeiting of currency or securities equivalent to currency foreseen in articles 262, 264 – to the extent that it refers to articles 262 and 267 – to the extent that it refers to articles 262 and 264 – of the Criminal Code;

f) Offences covered by a convention on the safety of air or maritime navigation.

Articles 57[35] and 58 Code of Penal Procedure govern interception of the communications of the defendant.

The suspect, according to Article 1 letter e Code of Penal Procedure, is "any person for whom there is evidence that he has committed or is preparing to commit a crime, or that he has participated in or is preparing to participate." Interception of communications may target any suspect, even if the identity of that person is not fully known.

43. Article 187 paragraph 4 Code of Penal Procedure also mentions the so-called intermediary. This is someone whose proximity to the suspect, such as family, friends, or any other relationship, may bring him into contact with the perpetrator of the crime, and when their communications may include matters relating to the crime under investigation. The intermediary is thus the person who receives or transmits messages intended for or coming from a defendant or a suspect.

This provision was introduced in the Code of Penal Procedure by Law 48/2007, of 29 August.[36] There is little doctrine or jurisprudence on this provision.

44. Finally, Article 187 paragraph 4 letter c Code of Penal Procedure allows the interception of communications of "a victim of a crime upon his/her effective or alleged consent." This is a particular case of interception, as consent of the target is requested to perform the interception.

The Code of Penal Procedure includes, in Article 67-A,[37] the definition of 'victim,' who is deemed to be a "natural person who has suffered damage, including an attack on his or her physical or mental integrity, emotional or moral damage, or property damage, directly caused by action or omission, in the context of crime," or any "relatives of a person whose death was directly caused by a crime and who have suffered damage as a result of that death."

This definition is clearly inspired by the definition included in Article 2[38] of the Directive 2012/29/EU of the European Parliament and of the Council, of 25 Octo-

---

[35] See Appendix.

[36] The Portuguese version of this law is available at http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=929&tabela=leis&ficha=1&pagina=1&so_miolo=

[37] Article 67-A was introduced by Law 130/2015, of 4 September 2015, that amended the Code of Penal Procedure, approved the status of the victim and transposed into national law the Directive 2012/29/EU, of the European Parliament and of the Council, of 25 October 2012, that established minimum standards on the rights, support, and protection of victims of crime – the Portuguese version of this act is available at https://dre.pt/web/guest/legislacao-consolidada/-/lc/106926276/201705261907/diploma?jp=true&did=70200875&rp=indice%2Fen

[38] Article 2 Definitions

1. For the purposes of this Directive the following definitions shall apply:

(a) 'victim' means:

ber 2012,[39] that established minimum standards on the rights, support, and protection of victims of crime.

Given that this is a relatively new provision, there has not yet been much interpretation of this clause, either in doctrine or jurisprudence.

6. Object of interception

45. As already noted, the original architecture of the framework respecting interception of communications was built on the existing reality in 1987,[40] which meant the interception of telephonic conversations.

Article 187 Code of Penal Procedure is included in Chapter IV (Telephone Tapping) and as per its original version applies to "interception and tape recording of telephone conversations or communications." Also, according to the first version, from 1987, Article 190 (referring to Article 187) allows interception of "any conversation or communication transmitted through any technical means other than a telephone device." Following the amendment of 2005, this Article 190 was converted into Article 189[41] and its scope was expanded.

To the mention of conversations or communications transmitted through any technical means other than a telephone was added "e-mail or other forms of telematic data transmission."

46. In this respect, it is useful to recall Article 18 Law on Cybercrime. In this article, the expression used is the same as in the Code of Penal Procedure: "intercept communications" in paragraph 1 and "interception and recording of transmissions of computer data" in paragraph 2.

Moreover, Article 18 paragraph 3 Law on Cybercrime states that the "interception may be intended for data on the content of communications or only to collect

---

(i) a natural person who has suffered harm, including physical, mental or emotional harm or economic loss which was directly caused by a criminal offence;

(ii) family members of a person whose death was directly caused by a criminal offence and who have suffered harm as a result of that person's death;

(b) 'family members' means the spouse, the person who is living with the victim in a committed intimate relationship, in a joint household and on a stable and continuous basis, the relatives in direct line, the siblings and the dependants of the victim;

(c) 'child' means any person below 18 years of age;

(d) 'restorative justice' means any process whereby the victim and the offender are enabled, if they freely consent, to participate actively in the resolution of matters arising from the criminal offence through the help of an impartial third party.

[39] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012L0029&from=PT

[40] The original version of the Code of Penal Procedure in force was published by *Decreto-Lei* 78/87, of 17 February 1987.

[41] See Appendix.

and recording traffic data; the judicial order referred above must specify the scope of the interception, according to the specific needs of the investigation."

47. No definition of *content data* can be found anywhere in these legal texts. However, the same is not true of *traffic data*. In fact, the Law on Cybercrime includes definitions in Article 2,[42] one of which is traffic data: "computer data relating to a communication made through a computer system, generated by this system as part of a chain of communication, indicating the origin of the communication, the destination, route, time, the date, size, duration or type of underlying service." This definition was borrowed from the corresponding provision of the Budapest Convention,[43] Article 1 d, in which traffic data is defined as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."

48. In conclusion, it can be said that within the Portuguese legal framework, everything in an electronic communication is interceptable: the content, or substance of the communication, but also all the information related to the transmission and transit of the message, while it is being broadcasted, or "alive." This covers all the technical related data.

Obtaining communications that have been transmitted and are already stored, as computer files in a storage medium, follows a different procedure (search and seizure of computer data), which is explored in section 73 of this chapter.

7. Procedures and operations

49. Article 188[44] Code of Penal Procedure describes the legal and technical process which must be observed by police, by the prosecutor, and by the judge, when performing interception of communications. However, Article 187 also includes rules that should be observed in this respect. Paragraph 6 determines the maximum term for interception of communications, stating that it shall be "authorised for a maximum time-limit of three months, renewable for equal periods, provided that the respective requirements for admissibility have been met."

50. As has already been noted, the initiative for an interception of communications belongs to the prosecutor (even if the police body has the possibility to suggest the measure). In face of this initiative, it is up to the judge to authorise it (or not) by the means of a written and reasoned order.

---

[42] See Appendix

[43] The official English version of the Budapest Convention is available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[44] See Appendix.

During this process, the police body is assisted by the service providers who, in practice, are informed by the police of the order issued by the judge and consequently, in response, provide the police body with access to all the communications of the target of the interception.

This procedure is only possible for those who provide their activity in the Portuguese territory – in other words, those who are authorised (by administrative authorities) to provide that activity in Portugal. If the required interception relates to a foreign provider, mutual legal assistance mechanisms must be used.

51. After access to communications has been permitted and facilitated by the provider, according to Article 188 Code of Penal Procedure, the responsibility to carry out all the practical steps in view of recording those communications belongs to the police body. According to Article 188 paragraph 1, the criminal police body is materially responsible for recording the communications and for producing a report pointing out the critical parts of the records (communications) which bear evidentiary relevance in the particular case. This report shall describe, in brief, the contents of the communications and shall explain their respective importance for the discovery of the truth in the case.

This report has a dual purpose: on the one hand, it identifies the relevant parts of the recorded communications, in view of obtaining evidence of the crimes under investigation. On the other hand, the report serves as a mechanism of control over the process. In fact, the police body carrying out the interception must present the prosecutor with such a report every fortnight (according to Article 188 paragraph 3 Code of Penal Procedure). The prosecutor in turn must submit the report to the judge within a maximum time limit of forty-eight hours. The purpose of this submission is to allow to the judge the effective control of the process of interception, providing him with regular information on its result and allowing him to intervene more actively, if necessary.

52. In fact, presenting this report fortnightly is mandatory for the police body who must also present the prosecutor (and the prosecutor must present the judge) with the technical devices (CD, USB flash disk, etc.) where the communications are recorded.

One should note the very short term given by the law to the prosecutor, to present the report to the judge, after receiving it from the police. With this very short term of just forty-eight hours, the law intends to make effective the judicial control of the process: a longer term would leave room for abuse and would weaken the protection of constitutional rights.

Article 188 Code of Penal Procedure also includes a clause concerning the effectiveness and efficiency of the judicial control: paragraph 5 states that, if required, the judge shall be technically assisted by the criminal police body and, if necessary, by an interpreter.

53. As a result of this judicial mechanism of control, it is supposed that the judge is aware of the interception process and the content of the particular case. However, it is not for the judge to select which parts of the communication are evidentially relevant in the case. In fact, because of the constitutional architecture of the system, this is the task of the prosecutor.

Thus, it is up to the prosecutor to decide which parts of the records of the intercepted communications are relevant. And only those parts selected by the prosecutor will be transcribed in the file and used as evidence for the purposes of the indictment[45] (Article 188 paragraph 9 letter a Code of Penal Procedure).

Of course, in an inquisitorial system, such as the Portuguese system, in the name of the contradictory principle, the defendant also has the legal possibility to request the transcription of certain parts of the communications, if not previously considered (Article 188 paragraph 9 letter b). An equivalent legal possibility is conferred by Article 188 paragraph 9 letter c), to the assistant party.[46]

54. These general rules have an exception and several *security valves*. The exception is foreseen in Article 188 paragraph 7 Code of Penal Procedure. According to this provision, the competence for the transcription and annexation to the proceedings of conversations and communications belongs to a judge, if the prosecutor wants to use those materials as evidence, for the specific purpose of justifying the application of provisional coercive or patrimonial guarantee measures. Thus, if during the investigation the prosecutor believes that a communication justifies, on solid grounds, the application of such a measure, he must request the transcription of such communications from the judge.

This is not the only possibility for the judge to influence the content of the interception. In fact, in materialising judicial control, Article 188 paragraph 6 Code of Penal Procedure allows the judge to destroy any part of the records of communications, once they are submitted to him, with the fortnightly report, which was mentioned above.

According to this paragraph, the judge shall "order the immediate destruction of the technical materials and reports clearly bearing no interest to the case at hand." The text of the law describes three particular types of communications that must be

---

[45] This rule is quite strict and imposes a burden on the prosecutor who must carefully choose the specific conversations or communications that will be used as evidence. A failure in this respect has the consequence that those communications cannot be used. The jurisprudence is clear on this. Along these lines, the ruling of *Tribunal da Relação* (Court of Appeal) from Porto of 13 May 2015 provides an example: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/e3e21d9e62cdb86f80257e520037f3a0?OpenDocument.

[46] In the Portuguese penal procedural system, the assistant party is a procedural subject whose interventions go a little further than the civil party, as in addition to being able to claim for civil compensation, as a result of a crime, he may also cooperate with the prosecutor in the construction of the penal case itself.

destroyed: one of them is recorded communications that do not involve anyone who may be an admissible target, as explained before. The second case of destruction refers to conversations or communications covering matters under secrecy (professional secrecy, public officials' secrecy or State secrecy). Finally, the judge shall also order the destruction of communications the disclosure of which might "seriously affect rights, liberties and guarantees." This latter clause is quite wide and open, allowing the judge to consider, on a case to case basis, which fundamental rights may, and may not, be affected by the use of a particular communication or conversation.

As stated, the judge is limited in this judgement to the materials and reports *clearly bearing no interest to the case*.

55. This is a quite well-balanced approach, providing room to the police and to the prosecutor to investigate and gather evidence of the crime but, on the other hand, requiring from the judge an intervening role. This role consists mainly in verifying, at least fortnightly, the regularity of the process of interception of communications, but also in suppressing undue records of the interception of communications, if those communications clearly do not relate to the facts under investigation.

This *interference* of the judge may be considered exceptional and a *security valve* of the system (it is not supposed to be used often). Normal proceeding, according to practice, is that within the fortnightly intervention, the judge issues an order, *authorising* the use of all the recorded communications.

56. The same exceptionality covers another important *security valve*, which ensures that the system of safeguards of the fundamental rights does not create entropies once an emergency occurs. In fact, the functioning of the system also includes another exceptional clause, in Article 188 paragraph 2. This provision allows the criminal police to take "knowledge of the contents of the intercepted communication in order to perform the investigative steps deemed necessary and urgent for purposes of ensuring any means of evidence." Thus, in urgent situations, the criminal police may use the content of communications, even before they are presented to the prosecutor (and the judge), that is, before the judicial control operates and outside the competence of the prosecutor, to decide which content should, or not, be considered for evidentiary purposes.

From the point of the view of the conception of the system, this legal possibility shall be used only exceptionally, when urgent situations occur (related to "ensuring any means of evidence"), as it is a distortion of the model.

8. Privileged information

57. As has been noted, the Portuguese Code of Penal Procedure considers interception of communications an exceptional investigative measure. It requires the

intervention of a judge, with the generic function of *authorising and controlling* the operation, in view of the respect of the legal safeguards and of the fundamental rights of the citizens.

One of the judicial powers described above concerns the destruction of recorded communications. The judge shall "order the immediate destruction of the technical materials and reports clearly bearing no interest to the case at hand," namely when the conversations or communications cover matters under secrecy (professional secrecy, public officials' secrecy or State secrecy) – Article 188 paragraph 6 Code of Penal Procedure.

However, this is not the only part of the procedural law concerning privileged information which deserves consideration.

58. In fact, with regard to the interception of communications between the defendant and his defence counsel the general principle is that it is not permitted – Article 187 paragraph 5 Penal Procedure Code. Exceptionally, however, it will be permitted if the judge has well-founded reasons to believe that those conversations may be an object or an element of a crime.

Thus, for the sake of the right of defence of the defendant, in principle, the interception of such kind of communications is not permitted, as it is assumed that those conversations may refer to the crime in the particular case or the defence strategy. However, in a situation when the defence counsel may be a co-perpetrator or a participant in a crime, the law exceptionally allows the interception of these communications.

59. A different situation will occur when there is need, within a criminal investigation, of intercepting communications where State authorities may intervene. This is the case with the President of the Republic, the President of the Assembly of the Republic (the Portuguese Parliament) or the Prime Minister.

In these cases, the general rules apply, regarding the admissibility of interception of communications. In fact, all of them may be included, occasionally, in one of the categories listed in Article 187 paragraph 4 Penal Procedure Code: they may be a suspect or defendant, they may be an intermediary (against whom there are grounds to believe they have received or transmitted messages aimed at, or coming from, the suspect or the defendant) and they may be a victim of a crime.

Thus, interception of communications is allowed in these cases.

The only special focus relates to the competent authority who must issue the competent order. Usually the judge in the particular area will be competent to issue the order. Regarding these State authorities, pursuant to Article 11 paragraph 2 letter b Code of Penal Procedure, it is a competence of the President of the Supreme Court of Justice "to authorize the interception, recording and transcription of conversations or communications with intervention of the Presidency of the Republic, the President of the Assembly of the Republic or the Prime Minister."

9. Generic approach of the Constitutional Court

60. The jurisprudence of the Constitutional Court with regard to interception of communications is not excessively rich.

This is most likely a consequence of the fact that most of the provisions of the Code of Penal Procedure were subject to preventive review of their constitutionality, by the Constitutional Court, even before it entered into force. In fact, in 1987 (the Code entered into force on 1 January 1988), the Constitutional Court had the opportunity to examine the draft code and to issue opinions[47] in this respect.

With regard to the interception of communications, Articles 187 and 190 were questioned, namely in view of the admissibility of the process of executing the interception of communications. The concerns regarding the compatibility with the Constitution referred to possible violations of Article 34 paragraph 4 Constitution (secrecy of telecommunications), of Article 26 paragraph 1 (namely regarding the aspects of privacy of the personal life and family life), and also of Article 18 paragraphs 2 and 3[48] (respecting the restriction of fundamental rights).

However, the Constitutional Court could not find any violation of the Constitution in the text of the Code of Penal Procedure. With regard to the interception of communications, the Constitutional Court decided that using this measure would be acceptable, in face of the nature and seriousness of certain crimes (those in which investigation of the interception of communications is allowed according to Article 187 Code of Penal Procedure).

10. Remedies

61. Article 190[49] Code of Penal Procedure provides for remedies for the infringement of the procedural rules respecting the interception of communications. Generally, it states that the "requirements and conditions referred to in articles 187, 188 and 189 are established under penalty of nullity," which means that if these conditions are not observed, the evidence obtained by the means of interception of communications will be null.

The doctrine considers this provision to be vague. In fact, the Code of Penal Procedure includes a complex system of nullities in Articles 118 to 123 – and this provision, Article 190, does not clarify exactly which type of nullity it refers to.

---

[47] The Constitutional Court issued the ruling 7/87, which decided that the challenged rules were not unconstitutional. This ruling is available, in Portuguese only, at https://dre.pt/application/file/a/257327

[48] See Appendix.

[49] See Appendix.

According to Articles 118 to 123, nullities *lato sensu* may be considered in the following categories: (i) irremediable nullities – Article 119, (ii) nullities dependent on argument – Articles 120 to 122, and (ii) mere irregularities – Article 123. An additional category is the evidentiary prohibition, referred to in Article 118 paragraph 3 and described in Article 126 Code of Penal Procedure.

The general principles, in this respect, are enshrined in Article 118 Code of Penal Procedure, which states that, within criminal procedure, the non-observance of the provisions of the law only determines the nullity of the act when it is expressly set forth in the law (paragraph 2). Moreover, in cases in which the law does not refer to nullity, the illegal act is merely irregular (paragraph 3).

This categorisation has significant consequences: the act which is merely irregular, according to Article 123 Code of Penal Procedure, may be repaired at the time it becomes known – and the irregular act will become valid.

Regarding nullities, those provided for in Article 119,[50] as mentioned before, are irremediable – and only these are irremediable. If an act is declared null, it will be invalid and void, as well as those acts that depend on it and those that it may affect, as stated in Article 122[51] paragraph 1 Code of Penal Procedure.

All the rest of the nullities provided for in the Code of Penal Procedures are considered nullities dependent on argument – Article 120. Even if the declaration of this type of nullity will have the same effect as the declaration of irremediable nullities, the rest of the regime is different. The major difference regards the need to argue such nullity. In fact, according to Article 121[52] Code of Penal Procedure, if the nullity is not argued, it will be healed. Thus, the act will become valid.

62. Portuguese doctrine considers that the non-observation of the rules regarding the admissibility of interception of communications, mainly provided for in Article 187 Code of Procedural Procedure (including the judicial order, or the justification of the need of the interception, or the requirements regarding the type of crime or the admissible targets) will be considered irremediable nullities.

Nullities dependent on argument are all those infringements of the rules regarding procedures and operations, namely those included in Article 188 Code of Penal Procedure. This is also the interpretation of the Supreme Court of Justice, in a ruling of 12 February 2018.

---

[50] See Appendix.

[51] See Appendix.

[52] See Appendix.

11. The conservation of records

63. The Code of Penal Procedure gives particular attention to the material result of interception of communications, that is, the records of communications, after they have been used to extract the relevant evidence.

As has already been observed, the main purpose of interception of communications is to record those communications, in view of obtaining evidence of a crime. According to the Code of Penal Procedure, the responsible entity for the process of recording the communications is the judicial police *(Polícia Judiciária)*, which must regularly present records to the prosecutor, in view of presenting them to a judge. Moreover, the judge has the duty to order the immediate destruction of the records, in specific cases, already mentioned, as provided for in Article 188 paragraph 6 Code of Penal Procedure.

In principle, according to Article 188 paragraph 7 Code of Penal Procedure, the relevant parts of those records should be subject to transcription in writing and used as evidence, by decision of the prosecutor (and, in a very specific case, as mentioned above, by order of the judge).

64. However, for reasons related to the principle of fair trial, after the decision of the prosecutor, the original records are kept and Article 188 paragraph 8 Code of Penal Procedure states that after the conclusion of the investigation ("upon conclusion of the inquiry stage"), both the assistant party and the defendant "may accede to the technical materials of the conversations or communications." The purpose of this provision is to allow both parties to acknowledge other parts of the communications, beyond those that were already subject to transcription. It also permits the eventual transcription of other parts, requiring to the judge to consider whether these additional parts of the communications are also admissible evidence. Paragraph 9 b and c of Article 188 refers to this possibility.

The possibility of accessing the content of the records is extended by Article 188 paragraph 11 Code of Penal Procedure to all those people whose conversations or communications have been intercepted.

This legal safeguard may be used until the end of the trial hearing, when a decision on the case is taken. After this decision becomes final and it is no longer possible to appeal, the records of communications which were not used as evidence (and transcribed) must be destroyed (as per Article 188 paragraph 13). The records of those communications that were used as evidence will be preserved, even when the decision becomes final. However, after this moment, they will be sealed "and may only be used should an extraordinary appeal be lodged."

The legal framework does not include a provision regarding the preservation or destruction of the communications recorded in cases where an indictment was not fulfilled (thus, that were filed by decision of the prosecutor). The practice within the Prosecution Service is to keep the records until the limitation period expires.

65. These are sensitive issues, from the point of view of privacy and violation of fundamental rights. In fact, on the one hand, destruction of records will prevent the content of communications from being disclosed, for example, publicly, when the secrecy of investigation ends. But on the other hand, in some cases, the destruction may jeopardise the position of the defendant.

Doctrine has considered Article 188 paragraph 6 Code of Penal Procedure, which states that the judge shall order the immediate destruction of the records of communications, in very specific cases. This *immediate destruction* may include communications that, at a later stage, would be useful, namely from the point of view of the defendant. However, such destruction will prevent the defendant from knowing its content. And moreover, the defendant is not consulted in this respect, nor can he react, for example, by appealing the order of the judge.

In this context, some authors state that a corrective reading of paragraph 6 must be made, to preserve its conformity with the Constitution. According to this doctrine, the judge shall order the destruction only after the investigation phases end and after the defendant has had access to all the produced evidence, including the records of communications.

12. The use of the records of the communications in other cases

66. The final question, regarding proceedings, concerns the use of the content of the intercepted communications for the purposes of other investigations. The issue is relevant, as during the interception of communications in view of obtaining evidence respecting to one crime, the investigators may realise that a particular communication may be useful evidence of another, different crime, being related to an already existing investigation, or obliging the opening of a new investigation.

Even if this interception of communications was valid, the record of its content cannot be directly used in other criminal investigations without due consideration. The Portuguese doctrine refers to this question as the *fortuitous knowledge* of relevant communications. The discussion does not relate to the admissibility of the interception, because that must have been questioned in the original case. The same can be said about the regularity of the proceedings. The question relates solely to the usability of this *fortuitous* information in a case other than the one in which it was obtained. And it is raised because of the limited and strict legal conditions which must be observed, when determining the execution of an interception of communications.

67. Historically, according to the Portuguese doctrine, it is clear that the use of this fortuitous information to open a new case, or within another already existing investigation, is limited to cases where interception of communications would be admissible. Namely, the use is limited to investigations of crimes included in the limited list provided for in Article 187 Code of Penal Procedure, but it is also per-

mitted if the person who was intercepted may be included in one of the limited categories of specific targets foreseen in the law.

The jurisprudence also requires that the *fortuitous* information must be of great interest to the investigation and that the defendant is able to exercise his rights, for example, accessing all the interceptions in a case, or requiring that other parts of the interception are taken into account, as evidence.

These are also the solutions found in Article 187 paragraph Code of Penal Procedure, that reads that the use of communications "cannot be used in the scope of any other proceedings (…) unless it has resulted from the interception of a means of communication used by the person referred to in paragraph 4 above and insofar as it proves to be indispensable for obtaining evidence of the crime set out in paragraph 1 above."

However, it must be noted that according to Article 187 paragraph 7 Code of Penal Procedure, the records of the communications may be used beyond the situations mentioned. In fact, if by the means of an interception of communications, the police body (or the prosecutor, or the judge) discovers or has notice of the existence of a crime, it will have the obligation to report that crime. In this case, the records of communications will not be considered as evidence of that crime, but mere notice of an infringement, which has yet to be proven, with other means of evidence.

C. Related Issues and Questions

1. Email and other electronic written communications

68. The Law on Cybercrime introduced in the domestic framework rules regarding search and seizure of computer data (on Articles 15 and 16), which are new procedural measures coinciding, in the cyberspace environment, with the classic forms of search and seizure.

But that act also introduced a special regime for the seizure of email and other electronic communications, as described in Article 17,[53] which clearly pretends to transpose to the digital environment the rationale of the seizure of correspondence, provided for in the Code of Penal Procedure,[54] but with several adjustments.

69. The first of the adaptations concerns the prior requirement – or not – of a judicial order determining the seizure of electronic communications. The law is not express, but nevertheless it is clear, assuming that a precautionary seizure of emails can be made even if there has been no previous judicial order to that effect. That is

[53] See Appendix.

[54] See Appendix.

what is stated in Article 17 Law on Cybercrime, when it is envisaged that the judge may authorise the seizure of messages that appear to be of great interest for the discovery of the truth or for evidence if they are discovered or found in the course of a computer search or other legitimate access to a computer system. If this is the case, then the judicial order must be issued after obtaining the records of the communications.

For the same reasons, it must be understood that the only legal requirement for the provisional seizure is the existence of a legitimate form of access to the computer on which they were stored.

This regime seeks to meet the practical requirements of real and concrete cases, allowing procedure to be more flexible in this regard. In fact, as a rule, email messages (and other types of written messages, with similar nature) are detected and seized in the course of a search, possibly of a physical location. As a rule, before a physical search, it is still unknown whether a computer will be found during its course, and it is even less clear whether such a computer will contain email messages. Lower still are the chances of predicting whether these messages may be of interest to the investigation. Real life shows that it would not be feasible to require, that the police, prior to any search, obtain judicial authorisation for the possibility of finding a computer in the course of the search and that such a computer would contain records of communications, and that such communications would be of evidentiary interest for the investigation of the case.

It is true that the legislator was not very clear on this point. However, no further interpretation of the law seems to be possible, other than that it allows for the provisional apprehension of emails in the course of a computer search, with the mere authorisation of a prosecutor – even if at a later stage such messages must be presented to a judge, in order to obtain a final authorisation to use the communications as evidence.

70. On the other hand, it is not required that the judge is the first to have knowledge of all the messages (as with physical correspondence, as required by Article 179 Code of Penal Procedure). On the contrary, it is the prosecutor who carries out the preliminary analysis of the relevant messages, only after which he submits them to the judge, in view of obtaining the authorisation to use them as evidence.

It should be noted that this regime, in Article 17, even if different, does not differ structurally from the one provided for in the Code of Penal Procedure for seizure of physical correspondence. In fact, Articles 179 and 252 Code of Penal Procedure establish the need to obtain prior judicial authorisation for *interception* of correspondence, but also allow for the provisional seizure of correspondence without prior judicial authorisation, if there is danger in the delay – this seizure must be validated by a judge at a later stage (Article 252 paragraph 3).

In any case, as has been noted, in the case of seizure of electronic communications, a judicial intervention is always required. It is always up to the judge to decide whether the use of the record of particular communication is admissible or not. Thus, in the framework of the Law on Cybercrime, emails and other electronic communications may never be seized and used as evidence in a particular case without an order from a judge to that effect.

2. Production order to provide computer data

71. Article 14[55] Law on Cybercrime describes the injunction for presentation or granting of access to data. This measure is not to be confused with the data preservation order or the order to expeditiously disclose traffic data.

In fact, it is an innovative provision, directly inspired by Article 18 of the Cybercrime Convention of the Council of Europe (Budapest Convention). The underlying reasons are the real difficulty experienced by law enforcement in the access to information when it is stored in computer systems, mainly as a consequence of the large storage capacity of modern systems and their enormous complexity. In the vastness of storage space of modern digital media, it can be very difficult and time consuming to find the information that is wanted if one does not have the collaboration of those who have availability and control over the system. Modern computer systems have immeasurable storage capacity and it is impossible for law enforcement – and undesirable, for many reasons – to trace all of its content. On the other hand, the various possibilities of hiding information or blocking access to it (for example, by encrypting or entering passwords to access file areas or documents) may require the collaboration of those who have control over it.

72. The injunction does not allow the refusal of cooperation of the person who has availability or control of the computer data – refusal to provide data will be punished as disobedience (final part of Article 14 paragraph 1 Law on Cybercrime).

However, its scope is limited and can never be addressed to a suspect or defendant in the proceedings in question (which is clear from Article 14 paragraph 5). Similarly, pursuant to paragraphs 6 and 7, the injunction may also not be used in respect of computer systems used for the exercise of professions subject to secrecy. The purpose of the law in this regard was to establish a regime consistent with the general safeguards of criminal proceedings in the protection of secrets.

---

[55] See Appendix.

3. Access to stored computer data

73. Search and seizure of computer data are generically covered by Articles 15 and 16 Law on Cybercrime. These are innovative provisions in content, but not in terms of the type of procedure they regulate. Article 15 provides for the searching for computer data and Article 16 provides for the seizure of computer data. In practice, these provisions have as their common goal to adapt to the digital environment and computer systems the classic search and seizure procedures.

By the means of computer search, described in Article 15 Law on Cybercrime, a form of coercive access was created to the computer medium which, as mentioned, is not really different from a physical search in the digital environment. In fact, the law (Article 15 paragraph 6) clearly and expressly states that the rules for the execution of the searches provided for in the Code of Criminal Procedure are applicable to this measure, of computer searches, in every element that is not expressly dealt with in Article 15, and with the necessary adaptations.

This is also the result of paragraphs 2 to 4 of Article 15 Law on Cybercrime, which contain material rules of the same nature as the regime of the physical searches, within the Code of Criminal Procedure.

The same solution is applicable for the regime for the seizure of computer data, provided for in Article 16, which establishes a regime similar to that of seizures, described in Articles 178 et seq. Code of Penal Procedure.

In both cases – computer searches and seizure of computer data – it is clear from the law that the power to order either procedure belongs to the *competent judicial authority* at each stage of the proceedings. Therefore, during the investigation, the competence is attributed to a prosecutor.

74. In both cases, safeguards were also established. In particular, Article 16 paragraph 5 Law on Cybercrime stipulates that seizure of computer data relating to computer systems used for the practice of legal advisory, or medical and banking activities, shall be subject, *mutatis mutandis*, to the restrictions, rules and formalities laid down in the Code of Penal Procedure. Likewise, professional or State secrecy prevail in this law.

On the other hand, the Law of Cybercrime shows concern to safeguard fundamental rights related to the privacy of those targeted by this type of investigation. In that sense, Article 16 paragraph 3 states that the intervention of a judge is always required whenever computer data containing information which is likely to reveal personal or intimate data which might jeopardise the privacy of the respective holder or third party is seized. In these situations, the computer data seized will be presented to the judge who will consider whether to admit it, taking into account the interests of the particular case. The non-observance of these legal formalities will result in the nullity of the obtained evidence.

75. With regard to this regime of computer search and to seizure of computer data, one additional note must be made: the rule introduced by Article 15 paragraph 5 Law on Cybercrime that allows the extension of the search to other computer systems must be highlighted. This includes, for example, situations in which the target of the search uses webmail, which is usually accessed from the targeted computer. In these cases, no one but the targeted person can access the relevant email account. There is probably no other way to access this account, unless there is a direct intervention in the moment. Article 15 paragraph 5 allows such an intervention, extending the search to the remote system – in this case, the webmail account.

This rule is partly inspired by Article 19 paragraph 2 of the Council of Europe Convention on Cybercrime (most commonly known as the Budapest Convention).

4. Covert actions and use of computer devices

76. The Portuguese law does not expressly allow the procedural measure normally known as *remote forensics*. That is, there is no express provision allowing authorities to lawfully access, remotely, the device of a suspect, using a particular piece of software. However, under the Law on Cybercrime, there is a provision on the neighborhood, allowing the use of computer devices when performing covert operations.

The admissibility and conditions for deploying covert operations are provided for in Law 101/2001, of 25 August 2001.[56] According to this act, covert actions are restricted to certain more serious types of crimes (described in detail in Article 2). Moreover, its execution is submitted to specific and mandatory procedural conditions (referred to in Article 3).

Article 19[57] Law on Cybercrime refers to covert operations. This provision, paragraph 1, extends the authorization to use covert actions to more types of crimes than those which are included in Law 101/2001. These are the specific types of crime foreseen in the Law on Cybercrime, but also any other crimes committed by means of a computer system, if they are punished with, at least, imprisonment of more than five years. Moreover, paragraph 1 extends the possibility of using covert actions in investigations of intentional crimes against sexual freedom and self-determination, or to cases where the victim is a minor, or in investigations of serious computer fraud, racial, religious, or sexual discrimination, economic and financial offenses, and crimes against *droit d'auteur*.

---

[56] The Portuguese version of this law is available at https://dre.pt/application/file/a/515573

[57] See Appendix.

In fact, one can say that the main purpose of Article 19 Law on Cybercrime is this enlargement of the scope of covert actions to investigations of *cyber related* or online crimes, in recognising the specificity of the environment where they occur and the particular difficulties of the respective investigation. Thus, Article 19 recognises online covert actions.

77. However, Article 19 paragraph 2 Law on Cybercrime contains another very significant provision. It states that it is permitted to use, within covert actions, *computer devices*. The letter of the law is not very detailed in this respect, but clearly allows the use of such type of means, "if it becomes necessary," and following, where applicable, "the same rules as for the interception of communications." In this paragraph, the Portuguese doctrine clearly sees a very synthetic regulation of the use of devices (including malware) to remotely access the device of a suspect. The main point in this respect is the applicability of the rules which are also applicable to the interception of communications.

However, this provision does not contain any rule referring to the operational aspects, or particular requisites of such operation. It also does not refer to the possible spectre of permitted activities and the technical rules that must be observed, when obtaining and recording data, as a result of the operation. Also, there are no rules regarding the particular case of using malware (regarding the type of malware, and its installation process, as well as the possible collection of information, among other aspects).

There is notice of the use of this process only in a very small number of cases. At the time of writing, there is not yet any jurisprudence on this topic.

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. General Internal Framework for Mutual Legal Assistance

78. Regarding international cooperation (understood within the framework of the formal mutual legal assistance), in general, Portugal has a clear approach: it has ratified all the treaties and conventions in this respect in force within the European space and also most global treaties covering these matters. Moreover, these international rules have been materialised at the domestic level with a national law on international cooperation in criminal matters.

Within Europe, Portugal ratified the European Convention on Mutual Assistance in Criminal Matters (the so-called Convention of 1959) and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000.

79. The Portuguese legal system includes a specific law regulating international judicial cooperation in criminal matters – Law 144/99,[58] of 31 August (amended by Law 104/2001, of 25 August, Law 48/2003, of 22 August, Law 48/2007, of 29 August, and Law 115/2009, of 12 October). This act regulates the international judicial cooperation process in criminal matters. Among other things, Law 144/99 allows the Portuguese national authorities to cooperate with foreign counterparts, providing for interception of communications in Article 160C.[59] In general, according to this article, the Portuguese authorities are authorised to perform interception of communications on behalf of authorities of a foreign State, on the grounds of an international agreement, treaty or convention and based on criteria provided for by the internal law, in view of similar circumstances.

According to the law, the national authority which is empowered to receive foreign requests for interception of communications is the *Polícia Judiciária*, the judicial police. However, as in any case under the domestic law, an authorisation of a national judge is required (paragraph 2). Thus, all the requests received by the *Polícia Judiciária* will be submitted to a judge for authorisation. The competent judge for such a case will be the judge of the *comarca* (district) of Lisbon.

After the issuance of the judicial order, the judicial police shall execute, as with all domestic interceptions, all the required actions and processes, in view of performing effectively the interception. Notwithstanding the process of judicial control of the interception, which follows the regular procedure, as provided for in national cases, it is the responsibility of *Polícia Judiciária* to fulfil all the tasks concerning transmitting the records of the interception of communications to the requesting State.

B. European Investigation Order

80. Portugal transposed into the national legal framework the provisions of the European Directive 2014/41/EU of the European Parliament and of the Council, of

---

[58] An English version of this law is available at http://gddc.ministeriopublico.pt/sites/default/files/documentos/pdf/act_144_99_31_august_international_judicial_coop_criminal_matters.pdf.

[59] Article 160C Interception of telecommunications

1. Upon request of the competent authorities of a foreign State, the interception of telecommunications effected in Portugal may be authorised, if such is provided for in an international agreement, treaty or convention and provided that in similar national circumstances interception would be admissible under the Portuguese criminal procedural law.

2. Polícia Judiciária shall be empowered to receive requests for interception; it shall thereupon submit the requests to the Criminal Investigations' judge of Lisbon for authorisation.

3. The decision concerning the authorisation mentioned in the preceding paragraph shall include an authorisation for the immediate transmission of the communication to the requesting State, should such transmission be provided for in the international agreement, treaty or convention under which the request was made.

3 April 2014, respecting the European Investigation Order in criminal matters, by Law 88/2017, of 21 August.[60] This domestic law includes a chapter (Chapter V), on interception of communications. Under this chapter, Article 42 describes, from the point of view of the requesting State, all the required conditions in view of issuing a European Investigation Order. Thus, it states the required conditions in view of requesting interception of communications, in the cases where there is a need of assistance of another State. Naturally, this framework is primarily applicable to the European Orders issued by Portuguese authorities, in view of seeking cooperation from the authorities in other States.

However, Article 42 also includes rules respecting the execution, by Portuguese authorities, of European Investigation Orders issued by other States – thus, in the perspective of the receiving State. These rules refer to grounds for refusal of the order (paragraph 5), practical conditions of execution (paragraph 6), and the respective cost (paragraph 11), among other things.

This article contains two very important references to other legal sources. On the one hand, in paragraph 9, it states that in the case of execution, within the Portuguese territory, of a European Investigation Order respecting interception of communication, Articles 187 to 190 Code of Penal Procedure will apply. That is, according to the Portuguese legal framework, all interceptions of communications shall respect the principles enshrined within the Code of Penal Procedure – including those interceptions executed on behalf of foreign authorities.

The other reference, in paragraph 10, states that if the European Investigation Order is in relation to computer data, the Law on Cybercrime will apply. That is, according to the domestic framework, the concrete executions of European Orders shall also follow the general principles of the domestic law, if the order relates to computer data.

C. Special Framework of the Law on Cybercrime

81. The Law on Cybercrime also includes provisions on international cooperation.

As explained above, the Law on Cybercrime is a special act, focusing on cybercrime and obtaining electronic evidence. This act describes special types of crimes, provides for specific investigative measures and also includes rules on international cooperation. Regarding the investigative rules, it must be noted that, according to Article 11, they apply to all criminal investigations that are committed by the

[60] A Portuguese version of this act is available at https://dre.pt/application/file/a/108029682

means of a computer system and to all cases where there is a need to collect electronic evidence.

Particularly in relation to international cooperation, Article 20[61] Law on Cybercrime states that the Portuguese national authorities "shall cooperate with foreign authorities for the purposes of criminal investigations or proceedings relating to computer systems or data, as well as the collection of evidence of a crime in electronic form." This is a general statement, defining the generic ability of the Portuguese authorities to fulfil requests from authorities of other States.

However, specifically referring to interception of communications, Article 26[62] Law on Cybercrime provides more concrete norms on the execution of international cooperation requests. It can be said that the legal regime under this article coincides with the already mentioned rules for cooperation described under Article 42 Law 88/2017, of 21 August (concerning the European Investigation Order). That is, even if the scope of the provisions are different, the material solutions of both of them coincide: Article 26 Law on Cybercrime applies to international cooperation requests concerning cybercrime or obtaining electronic evidence; Article 42 Law 88/2017, of 21 August has a narrower scope, as it concerns only those cooperation requests that have the format of a European Investigation Order. However, the specific rules and principles enshrined in both provisions coincide, simply in parallel regimes.

Following the general guidelines of the system, the intervention of a judge is always required, and cooperation is only provided "since it is stipulated by a treaty or an international agreement and whether it is a case where such interception is allowed (…), in a similar national case."

82. Moreover, regarding practical aspects, Article 26 also states, in paragraph 2, that the national authority responsible for receiving international requests in view of intercepting communications is the *Polícia Judiciária*, which has the duty to report the case to a prosecutor, so the request "can be presented to the judge in charge of the comarca of Lisbon for authorization."

As regards the transmission of data (obtained through the interception of communications), the Portuguese law is vague and refers to existing international treaties on this aspect. In fact, Article 26 paragraph 4 Law on Cybercrime states that the judicial order that authorises the execution of the interception of communications "also allows the immediate transmission of the communication to the requesting State, if such a procedure is foreseen in a treaty or an international agreement under which the request is made." A parallel solution is found in Article 160C[63] of

---

[61] See Appendix.

[62] See Appendix.

[63] See note 59.

Law 144/99 (on international cooperation, as explained above), paragraph 3 of which is quite similar to Article 26 paragraph 4 Law on Cybercrime.

These options follow the provisions of the Directive 2014/41/EU of the European Parliament and of the Council, of 3 April 2014, respecting the European Investigation Order in criminal matters. In fact, in Article 30 paragraph 1, the Directive foresees the possibility of issuance of a European Investigation Order to intercept communications. Moreover, in paragraph 5, requirements for the execution of the order are defined, as well as reasons for refusal. Namely, in this respect, it is stated that the requisites of interception of communications, as defined by the national law, applicable to a similar national case, may apply.

Finally, Article 26 paragraph 4 states that this regime (namely respecting the general conditions provided for in paragraph 1), "shall apply, *mutatis mutandis*, to requests made by Portuguese judicial authorities" to the authorities of other States.

Appendix

Legislation

Constitution of the Republic of Portugal

Article 18 Legal force

1 The constitutional precepts with regard to rights, freedoms and guarantees are directly applicable and are binding on public and private entities.

2 The law may only restrict rights, freedoms and guarantees in cases expressly provided for in the Constitution, and such restrictions must be limited to those needed to safeguard other constitutionally protected rights and interests.

3 Laws that restrict rights, freedoms and guarantees must have a general and abstract nature and may not have a retroactive effect or reduce the extent or scope of the essential content of the constitutional precepts.

Article 26 Other personal rights

1. Everyone is accorded the rights to personal identity, to the development of personality, to civil capacity, to citizenship, to a good name and reputation, to their image, to speak out, to protect the privacy of their personal and family life, and to legal protection against any form of discrimination.
2. The law shall lay down effective guarantees against the improper procurement and misuse of information concerning people and families and its procurement or use contrary to human dignity.

Article 32 Safeguards in criminal procedure

1. Criminal procedure shall ensure all the safeguards of the defence, including the right to appeal.
2. Every accused person is presumed innocent until the sentence in which he was convicted has transited in rem judicatam and must be tried as quickly as is compatible with the safeguards of the defence.

3. Accused people have the right to choose counsel and to be assisted by him in relation to every procedural act. The law shall specify those cases and phases of procedure in which the assistance of a lawyer is mandatory.
4. All committal proceedings shall be the competence of a judge, who may, as laid down by law, delegate the practice of such committal-related acts as do not directly concern fundamental rights to other entities.
5. Criminal procedure shall possess an accusatorial structure, and trial hearings and the committal-related acts that are required by law shall be subject to the adversarial principle.
6. The law shall define the cases in which, subject to the safeguarding of the rights of the defence, the presence of the accused person at procedural acts, including trial hearings, may be dispensed with.
7. Victims have the right to intervene in the proceedings, as laid down by law.
8. All evidence obtained by torture, coercion, infringement of personal physical or moral integrity, or improper intromission into personal life, the home, correspondence or telecommunications is null and void.
9. No case may be withdrawn from a court that was competent under a pre-existing law.
10. Accused people in proceedings concerning administrative offences or in any proceedings in which sanctions may be imposed are assured the right to be heard and to a defence.

Article 34 Inviolability of home and correspondence

1 Domiciles and the secrecy of correspondence and other means of private communication are inviolable.

2 Entry into a citizen's domicile against his will may only be ordered by the competent judicial authority and then only in the cases and in compliance with the forms laid down by law.

3 No one may enter any person's domicile at night without his consent, save in situations of flagrante delicto, or with judicial authorisation in cases of especially violent or highly organised crime including terrorism and trafficking of human beings, arms or narcotics, as laid down by law.

4 The public authorities are prohibited from interfering in any way with correspondence, telecommunications or other means of communication, save in the cases in which the law so provides in matters related to criminal procedure.

Article 35 Use of information technology

1 Every citizen has the right of access to all computerised data that concern him, which he may require to be corrected and updated, and the right to be informed of the purpose for which they are intended, as laid down by law.

2 The law shall define the concept of personal data, together with the terms and conditions applicable to its automatized treatment and its linkage, transmission and use, and shall guarantee its protection, particularly by means of an independent administrative entity.

3 Information technology may not be used to treat data concerning philosophical or political convictions, party or trade union affiliations, religious faith, private life or ethnic origins, save with the express consent of the data subject, or with an authorisation provided for by law and with guarantees of non-discrimination, or for the purpose of processing statistical data that are not individually identifiable.

4 Third-party access to personal data is prohibited, save in exceptional cases provided for by law.

5 The allocation of a single national number to any citizen is prohibited.

6 Everyone is guaranteed free access to public-use information technology networks. The law shall define the regime governing cross-border data flows, and the appropriate means for protecting both personal data and other data whose safeguarding is justified in the national interest.

7 Personal data contained in manual files enjoy the same protection as that provided for in the previous paragraphs, as laid down by law.

Article 205 Court decisions

1 Court decisions that are not merely administrative in nature shall set out their grounds in the form laid down by law.

2 Court decisions are binding on all public and private entities and prevail over the decisions of any other authorities.

3 The law shall regulate the terms under which court decisions are executed in relation to any authority and shall lay down the sanctions to be imposed on those responsible for any failure to execute them.

Code of Penal Procedure

Article 57 The status of defendant

1 Any person formally charged or against whom the beginning of the examining stage has been requested in the scope of criminal proceedings shall acquire the status of defendant.

2 The defendant's status shall remain valid during all stages of proceedings.

3 The provisions of Article 58 paragraphs 2 to 6, shall apply accordingly.

Article 58 Acquiring the status of defendant

1 Subject to the provisions of Article 57, the formal acquisition of the status of defendant is mandatory as soon as:

a) A person makes statements before any judicial authority or criminal police body during an inquiry started against him, where there are grounds to suspect that such person has committed a criminal offence;

b) A coercive or patrimonial guarantee measure must be imposed on a specific person;

c) A suspect is arrested under the terms and for the purposes of Articles 254 to 261 of this Code; or

d) A police report has been drawn up identifying a person as an alleged offender and such person has been informed on the contents thereof, unless the report is clearly ungrounded.

2 The status of defendant is acquired by the communication to the concerned person, either orally or in writing, by a judicial authority or criminal police body that, as of that moment, he has the status of defendant in criminal proceedings and, if necessary, by the explanation of procedural rights and duties of defendants laid down in Article 61, which he, therefore, is bound to observe.

3 The status of defendant following communication by a criminal police body is reported to the judicial authority within 10 days. The judicial authority shall have a 10-day period for examination and validation or non-validation of the act.

4 The status of defendant implies the handing over to the concerned person, if possible, simultaneously, of a document specifying the particulars of the case and those of his defence counsel, should the latter have been appointed. The document must also indicate the defendant's procedural rights and duties as listed in Article 61.

5 Failure to comply with, or breach of, the formalities laid down in the preceding paragraphs shall prevent the use as evidence of any statements made by the concerned person.

6 The non-validation of the status of defendant by the judicial authority does not affect evidence previously collected.

Article 119 Irremediable nullities

The following are Irremediable nullities, which must be officially declared at any stage of the proceedings, in addition to those which are provided for in other legal provisions:

a) The lack of the number of judges or jurors that must constitute the court, or the violation of the legal rules regarding the way of determining their composition;

b) The lack of promotion of the process by the prosecutor, in accordance with Article 48, as well as its absence to acts for which the law requires the respective appearance;

c) The absence of the accused or his counsel, in cases in which the law requires the appearance of the accused;

d) The lack of investigation or investigation, in cases in which the law determines its obligatoriness;

e) Breach of the jurisdiction rules of the court, without prejudice to the provisions of Article 32 paragraph 2;

f) Employment of a special process outside the cases provided by law.

Article 121 Healing of nullities

1 Except in cases where the law provides otherwise, nullities are remedied if the procedural participants concerned:

a) Expressly renounce to argue them;

b) Have expressly accepted the effects of the annulled act; or

c) If they have prevailed of the faculty whose exercise the voidable act was directed.

2 The nullities relating to lack or vice of notification or summons to procedural act will be remedied if the interested person attends or waives to attend the act.

3 Exempt from the provisions of the preceding paragraph the cases in which the interested party only appears with the intention to argue the nullity.

Article 122 Effects of a declaration of nullity

1 Nullities render invalid the act in which they occur, as well as those that depend on it and those that may affect.

2 The declaration of nullity determines which acts are considered to be invalid and orders, whenever necessary and possible, their repetition, putting the respective expenses in charge of the defendant, the assistant or civil parties that have given cause, wrongfully, to nullity.

3 When declaring a nullity, the judge takes advantage of all acts that can still be saved from the effect of that.

Article 126 Prohibited methods of obtaining evidence

1 Evidence obtained through torture, coercion or, in general, offense to the physical or moral integrity of people shall be null and void and may not be used.

2 It is offensive to the physical or moral integrity of the people, the evidence obtained, even with their consent, through:

a) Disturbance of freedom of will or decision through mistreatment, bodily injury, administration of means of any nature, hypnosis or use of cruel or deceptive means;
b) Disturbance by any means of memory or evaluation capacity;
c) Use of force, outside the cases and limits allowed by law;
d) Threat with a legally inadmissible measure and, as well, with denial or conditioning of obtaining a legally established benefit;
e) Pledge of legally inadmissible advantage.

3 Except for cases provided for by law, evidence obtained through intrusion in private life, at home, in correspondence or in telecommunications without the consent of the respective holder is also null and void.

4 If the use of the methods of obtaining evidence provided for in this article constitutes a crime, they may be used for the exclusive purpose of proceeding against the agents of the same.

Article 179 Seizure of correspondence

1 Under penalty of nullity, the judge may authorize or order, by order, seizure of letters, orders, values, telegrams or any other correspondence, even at the post offices and telecommunications, where there are reasonable grounds to believe that:
a) The correspondence was issued by the suspect or addressed to him, even if under a different name or through a different person;
b) It is in case a crime punishable by a maximum prison sentence of 3 years; and
c) The diligence will be of great interest for the discovery of the truth or for obtaining the evidence.

2 The seizure and any other form of control of the correspondence between the suspect and his counsel is prohibited, under penalty of nullity, unless the court has reasonable grounds to believe that the correspondence may be an object or element of a crime.

3 The judge who authorized or ordered the proceeding is the first person to be aware of the contents of the seized correspondence. If he considers it relevant to the case, it will be annexed to the file; if it does not, he will release it to the right person, and he it will not be used as evidence, being bound by a duty of secrecy in relation to what he has learned and is not related to the case.

Article 187 Admissibility

1 Interception and tape recording of telephone conversations or communications may only be authorized during the inquiry where there are grounds for believing that this step is indispensable for the discovery of the truth or that the evidence would, by any other means, be impossible or very hard to collect. Such authorization shall be granted by means of a reasoned order issued by the Examining Judge and upon the request of the Public Prosecution Service, as regards the following criminal offences:
a) Criminal offences to which a custodial sentence with a maximum limit over three years applies;
b) Drug-related offences;
c) Possession of a prohibited weapon and illicit trafficking in weapons;
d) Smuggling offences;
e) Insult, threat, coercion, disclosure of private life and disturbance of the peace and quiet, whenever committed by means of a telephone device;
f) Threat with the commission of a criminal offence or abuse and simulation of danger signals; or

g) Escape from justice, whenever the defendant has been sentenced for a criminal offence foreseen in the preceding sub-paragraphs.

2 The authorization provided for in paragraph 1 above may be requested to the judge with jurisdiction over the locations from where the telephone conversation or communication is likely to be effected, or over the central office of the entity competent to conduct the criminal investigation, when dealing with the following criminal offences:

a) Terrorism, violent or highly organized criminality;

b) Illegal restraint, kidnapping and taking of hostages;

c) Offences against cultural identity and personal integrity, as provided for in Book II, Title III, of the Criminal Code and in the Criminal Law on Violations of International Humanitarian Law;

d) Offences against State security foreseen in Book II, Title V, Chapter I, of the Criminal Code;

e) Counterfeiting of currency or securities equivalent to currency foreseen in articles 262, 264 – to the extent that it refers to articles 262 and 267 – to the extent that it refers to articles 262 and 264 – of the Criminal Code;

f) Offences covered by a convention on the safety of air or maritime navigation.

3 In the cases foreseen in the preceding paragraphs, the authorization is communicated within a seventy-two hour period to the judge to whom the case was referred, who is responsible for carrying out the subsequent jurisdictional acts.

4 Regardless of the entity who owns the means of communication used, both the interception and the recording referred to in the preceding paragraphs can only be authorised against:

a) The suspect or the defendant;

b) Any person acting as an intermediary, against whom there are grounds to believe that he/she receives or transmits messages aimed at, or coming from, the suspect or the defendant; or

c) A victim of a crime upon his/her effective or alleged consent.

5 No interception and recording of telephone conversations or communications between the defendant and his defence counsel is allowed unless the judge has reasonable grounds to believe that the said conversation or communication is the object or the constitutive element of a criminal offence.

6 The interception and the recording of any conversations or communications are authorised for a maximum time-limit of three months, renewable for equal periods, provided that the respective requirements for admissibility have been met.

7 Without prejudice to article 248, the recording of conversations or communications cannot be used in the scope of any other proceedings, either on-going or to be instituted, unless it has resulted from the interception of a means of communication used by the person referred to in paragraph 4 above and insofar as it proves to be indispensable for obtaining evidence of the crime set out in paragraph 1 above.

8 In the cases provided for in paragraph 7 above, the technical means in which conversations or communications have been recorded, as well as the decisions having clearly stated the need for the interceptions are enclosed, following a judge's ruling, to the proceedings in the scope of which they are to be used as evidence. If necessary, copies thereof shall be made

Article 188 Formalities of the operations

1 The criminal police body carrying out the interception and the recording referred to in the preceding article draws up the respective records and produces a report pointing out

the parts which bear relevance to the evidence, describing in brief the respective contents and explaining the respective importance for the discovery of the truth.

2 The provisions set forth in the preceding paragraph do not prevent the criminal police body responsible for the investigation from having previous knowledge of the contents of the intercepted communication in order to perform the investigative steps deemed necessary and urgent for purposes of ensuring any means of evidence.

3 The criminal police body mentioned in paragraph 1 above provides the Public Prosecution Service, every fortnight counted from the first interception made, with the respective technical material, as well as with the respective records and reports.

4 The Public Prosecution Service submits the elements mentioned in the preceding paragraph to the judge within a maximum time limit of forty-eight hours.

5 In order to become acquainted with the content of the conversations or communications, the judge shall be assisted, whenever appropriate, by a criminal police body and shall appoint, if necessary, an interpreter.

6 Without prejudice to the provisions set forth in paragraph 7 of the preceding article, the judge shall order the immediate destruction of the technical materials and reports clearly bearing no interest to the case at hand:

a) Concerning conversations between people not referred to in paragraph 4 of the preceding article;

b) Covering matters under professional secrecy, under secrecy binding officials or under State secrecy; or

c) The disclosure of which may seriously affect rights, liberties and guarantees; and all interveners in the operations shall be bound by the duty of secrecy as to what has been disclosed through the said conversations.

7 During the inquiry, the judge shall order, upon the request of the Public Prosecution Service, the transcription into and annexation to the proceedings of the conversations and communications which, on solid grounds, justify the application of coercive or patrimonial guarantee measures, with the exception of the Statement of Identity and Residence.

8 Upon conclusion of the inquiry stage, both the party assisting the Public Prosecutor and the defendant may accede to the technical materials of the conversations or communications and obtain, at their own expense, copies of the parts which they intend to transcribe for purposes of annexation to the case, as well as of the reports foreseen in paragraph 1 above, until the expiry of the time-limits given for purposes of requesting the opening of the preliminary judicial stage or for purposes of producing the defence statement.

9 Conversations or communications that can be used as evidence are only those which:

a) The Public Prosecution Service orders the criminal police body responsible for the interception and recording to transcribe and which have been pointed out in the indictment as being means of evidence;

b) The defendant transcribes from the copies foreseen in the preceding paragraph and encloses to the application for the opening of the preliminary judicial stage or to the production of the defence statement; or

c) The party assisting the Public Prosecutor transcribes from the copies foreseen in the preceding paragraph and encloses to the case within the time limit foreseen for requesting the opening of the preliminary judicial stage, even if such a party does not request the said opening or has no legitimacy to do so.

10 The court may hear the recordings so as to determine the correction of the transcriptions already made or the respective annexation to the proceedings of new transcrip-

tions, whenever needed for purposes of discovering the truth and of giving a just decision on the case.

11 The people whose conversations or communications have been heard and transcribed may examine the respective technical materials until the closure of the trial hearing.

12 The technical materials concerning conversations or communications which are not transcribed for purposes of being used as means of evidence are kept inside sealed envelopes, upon an order by the court, and destroyed after the decision on the case has acquired legal force.

13 After the decision has become final, as mentioned in the preceding paragraph, the technical materials which have not been destroyed shall be kept inside a sealed envelope, enclosed to the proceedings, and may only be used should an extraordinary appeal be lodged.

Article 189 Scope

1 The provisions laid down in articles 187 and 188 shall apply accordingly to any conversation or communication transmitted through any technical means other than a telephone device, in particular by e-mail or other forms of telematics data transmission, even if kept under a digital medium, and to the interception of the communications between people present.

2 Obtaining and enclosing to the proceedings data regarding mobile phone tracing or records of conversations or communications may only be ordered or authorized, regardless of the stage of the proceedings, by means of an order issued by the judge, as regards criminal offences foreseen in article 187(1) and the people mentioned in article 187(4).

Article 190 Nullity

The requirements and conditions referred to in articles 187, 188 and 189 are established under penalty of nullity.

Law on Cybercrime (Law 109/2009)

Article 2 Definitions

For the purposes of this Law:

a) 'computer system' means any device or set of connected or related devices, in which one or more of these produces, running a program, the automated processing of data, and the network that supports communication between them and the set of data stored, processed, retrieved or transmitted by that or those devices, with a view to its operation, use, protection, and maintenance;

b) 'computer data' means any representation of facts, information or concepts in a format capable of being processed by means of a computer system, including programs able to make a computer system to perform a function;

c) 'traffic data' means computer data relating to a communication made through a computer system, generated by this system as part of a chain of communication, indicating the origin of the communication, the destination, route, time, the date, size, duration or type of underlying service;

d) 'service provider' means any entity, public or private, that provides users of its services the ability to communicate through a computer system and any other entity that stores computer data on behalf and of that service or its users;

e) 'interception' means the act intended to capture information in a computer system, using electromagnetic devices, acoustic, mechanical, or other;

f) 'topography', a series of images linked together, regardless of how they are fixed or encoded, representing the three-dimensional configuration of the layers that make up a semiconductor product and in which each image reproduces the drawing, or part of a surface of the semiconductor product, whatever stage of their manufacture;

g) 'semiconductor product' means the final or intermediate form of any product, comprising a substrate that includes a layer of semiconductor material and comprising one or more layers of conductive, insulating or semiconducting, according to the arrangement to a three-dimensional configuration and intended to fulfil, exclusively or not, an electronic function.

Article 11 Scope of procedural provisions

1 Except as provided in Articles 18 and 19, the procedural provisions of this chapter shall apply to proceedings relating to crimes:

a) Described under this Law;

b) Committed by means of a computer system, or

c) When it is necessary to collect evidence in electronic form.

2 The procedural provisions of this Chapter shall not affect the rules of Law No. 32/2008 of 17 July.

Article 14 Injunction for providing data or granting access to data

1 If during the proceedings it becomes necessary for the gathering of evidence in order to ascertain the truth, obtain certain and specific data stored in a given system, the judicial authority orders to the person who has the control or availability of those data to communicate these data or to allow the access to them, under penalty of punishment for disobedience.

2 The order referred to in the preceding paragraph identifies the data in question.

3 In compliance with the order described in paragraphs 1 and 2, whoever has the control or availability of such data transmits these data to the competent judicial authority or allows, under penalty of punishment for disobedience, the access to the computer system where they are stored.

4 The provisions of this Article will apply to service providers, who may be ordered to report data on their customers or subscribers, which would include any information other than the traffic data or the content data, held by the service provider, in order to determine:

a) The type of communication service used, the technical measures taken in this regard and the period of service;

b) The identity, postal or geographic address and telephone number of the subscriber, and any other access number, the data for billing and payment available under a contract or service agreement, or

c) Any other information about the location of communication equipment, available under a contract or service agreement.

5 The injunction contained in this article may not be directed to a suspect or a defendant in that case.

6 The injunction described under this article is not applicable to obtain data from a computer system used within a legal profession, medical, banking, and journalists' activities.

7 The system of professional secrecy or official and State secrets under Article 182 of the Code of Criminal Procedure shall apply mutatis mutandis.

Article 17 Seizure of email communications and records of communications of similar nature

If during a search or other legitimate access to a computer system, emails or records of communications of a similar nature are found, stored in this system or in another system where it is legitimately allowed the access from the first, the judge may authorize or order, the seizure of those records who appear to have a great interest to establish the truth, applying the corresponding rules of the seizure of correspondence of the Code of Criminal Procedure.

Article 18 Interception of communications

1 It is allowed to intercept communications in proceedings relating to crimes:
   a) Described under this Act, or
   b) Committed by the means of a computer system or, when it is necessary to gather evidence in electronic form if such crimes are described in Article 187 of the Code of Criminal Procedure.

2 The interception and recording of transmissions of computer data can only be allowed during the investigation, by founded decision of the judge or by request of the Prosecution Service, if there are reasons to believe that this is essential to establish the truth or that gathering the evidence would otherwise be impossible or very difficult to obtain by other means.

3 The interception may be intended for data on the content of communications or only to collect and recording traffic data; the judicial order referred above must specify the scope of the interception, according to the specific needs of the investigation.

4 Respecting all the aspects not described under this article, the interception and recording of transmissions of computer data are subject to the general regulation on interception and recording conversations or telephone conversations contained in Articles 187, 188 and 190 of the Code of Criminal Procedure.

Article 19 Under covered actions

1 It is allowed to make use of under covered actions under Law No 101/2001 of 25 August, in the manner specified therein, in the course of investigations concerning the following crimes:
   a) Described under this law;
   b) Committed by means of a computer system, if they are punished with, at least, imprisonment of more than 5 years or, even if the abstract penalty is inferior, the act is intentional and respects to crimes against sexual freedom and self-determination, or to cases in which the victim is a minor, or in cases of serious fraud, computer and communications fraud, racial, religious or sexual discrimination, economic and financial offenses, and crimes set out under Title IV of the Code of Copyright.

2 If it becomes necessary the use computer devices, it must follow, when applicable, the same rules as for the interception of communications.

Article 20 International cooperation

The national authorities shall cooperate with the competent foreign authorities for the purpose of criminal investigations or proceedings relating computer systems or data, as well as the collection of evidence of a crime in electronic form, according to the rules on transfer of personal data contained in Law No 67/98 of 26 October.

Article 26 Interception of communications within international cooperation

1 Pursuant to a request by the competent foreign authority it may be authorized by the judge the interception of computer data transmissions from a computer system located in Portugal, since it is stipulated by a treaty or an international agreement and whether it is a case where such interception is allowed under Article 18, in a similar national case.

2 Polícia Judiciária is the responsible entity for receiving requests to intercept communications, which report to the Public Prosecution Service, so as they can be presented to the judge in charge of the comarca of Lisbon for authorization.

3 The referred order of authorization also allows the immediate transmission of the communication to the requesting State, if such a procedure is foreseen in a treaty or an international agreement under which the request is made.

4 The provisions of paragraph 1 shall apply, mutatis mutandis, to requests made by Portuguese judicial authorities.

Bibliography

Albuquerque, Paulo Pinto, "*Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*", Universidade Católica Portuguesa Editora. Lisboa 2009.

Andrade, Manuel da Costa, "*Bruscamente no Verão Passado – A reforma do Código de Processo Penal, observações críticas sobre uma lei que podia e devia ter sido diferente*", Coimbra Editora. Coimbra 2009.

– "*Das Escutas Telefónicas*," in "*Congresso de Processo Penal*," coordenação de Manuel Monteiro Guedes Valente, Almedina. Coimbra 2005.

– "*Sobre o regime processual penal das escutas telefónicas*," in "*Revista Portuguesa de Ciência Criminal*", Ano I, nº 3, Coimbra Editora. Coimbra 1991.

Cunha, José Manuel Damião da, "*O Regime Legal das Escutas telefónicas – algumas breves reflexões*," in "*Revista do CEJ – Jornadas sobre a revisão do Código de Processo Penal*," nº 9 (especial), CEJ. Lisboa 2008.

Leite, André Lamas, "*As Escutas Telefónicas – algumas reflexões em redor do seu regime e das consequências processuais derivadas da respetiva valoração*", in "*Revista da Faculdade de Direito da Universidade do Porto*", Ano I, Coimbra Editora. Coimbra 2004.

– "*Entre Péricles e Sísifo: o Novo Regime Legal das Escutas Telefónicas*", in "*Revista Portuguesa de Ciência Criminal*", Ano 17, nº 4, Coimbra Editora. Coimbra 2007.

Lopes, José Mouraz, "*Escutas telefónicas: seis teses e uma conclusão*," in "*Revista do Ministério Público*," Ano 26, nº 104, Sindicato dos Magistrados do Ministério Público. Lisboa 2005.

Masquita, Paulo Dá, "*Processo Penal, Prova e Sistema Judiciário*," Coimbra Editora. Coimbra 2010.

Ribeiro, Cristina, "*Escutas Telefónicas: Pontos de Discussão e Perspetivas de Reforma*," in "*Revista do Ministério Público*," Ano 24, nº 96, Sindicato dos Magistrados do Ministério Público. Lisboa 2003.

Rodrigues, Benjamim Silva, "*A Monitorização dos Fluxos Informacionais e Comunicacionais*," volume I, Coimbra Editora. Coimbra 2009.

Teixeira, Carlos Adérito, "*Escutas Telefónicas – a mudança de paradigma e os velhos e os novos problemas*," in "*Revista do CEJ – Jornadas sobre a revisão do Código de Processo Penal*," nº 9 (especial). Lisboa 2008.

Spain*

National Rapporteur:
Lorena Bachmaier Winter

* This report reflects legislation and case law as of January 2019.

Contents

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Security Services with Powers of Telecommunication Interception

1. National security architecture

For understanding the gathering of information through the interception of telecommunications, it is not necessary to enter into details regarding the precise regulation of all the departments, bodies, and units that may be in some or another way involved in the national security field. The Spanish national security "architecture" follows a quite simple structural pattern:

- State Security Intelligence Service, the National Intelligence Centre (*Centro Nacional de Inteligencia*, CNI), and the criminal prosecution;
- Ministry of Interior: law enforcement, criminal policies, and public security and criminal prevention functions;
- Ministry of Defence: military intelligence for external threats and national defence (*Centro de Inteligencia de las Fuerzas Armadas*, CIFAS);
- Criminal Prosecution: judiciary and public prosecution service. The judicial police are formally part of the Ministry of Interior, but functionally, when carrying out criminal investigations, they are subject to the instructions of the judges.

The legal framework and their precise powers with regard to the interception of telecommunications will be explained below.

2. Powers for the interception of telecommunication

a) Law of criminal procedure

Article 588 of the Spanish Criminal Procedure Code (*Ley de Enjuiciamiento Criminal*, LECRIM), as of 5 October 2015 provides for the general legal framework on interception of telecommunications regarding the investigation of criminal offences within the criminal procedure. The general threshold for these interceptions is: offences sanctioned with a penalty higher than three years imprisonment, or organised crime, terrorism and cybercrime. The regulation will be explained in detail below.

b) Preventive law

The Spanish system does not allow for the interception of communications within the preventive law. So-called pro-active investigative measures are prohibited. This prohibition is now specifically stated under **Article 588*bis* a. LECRIM**:

> 2. The principle of speciality requires that the investigative measure is related to the investigation of a specific offense. No IT investigative measures may be authorized aimed at preventing a crime nor for discovering it or confirm suspicions that have not an objective foundation.

Prior to this rule, the Supreme Court had repeatedly stated that interception of communications without enough probable cause of a concrete offence are unlawful.[1]

c) Law of intelligence agencies

The activities of the CNI (*Centro Nacional de Inteligencia*, National Intelligence Centre) are regulated by Law 11/2002.[2] Article 4 lists the functions of the CNI. For the fulfilment of its objectives, the CNI has the following functions (paragraph b):

> To prevent, detect, and enable the neutralization of those activities of foreign services, groups or individuals that endanger, threaten, or violate the constitutional order, rights and freedoms of European citizens, sovereignty, integrity, and security of the state, the stability of its institutions, national economic interests and welfare of the population.

The prevention of criminal offences such as terrorism, organised crime, and cybercrime fall within this provision.

Organic Law 2/2002[3] regulates the interception of communications by the CNI. Previously, the Supreme Court had convicted several agents for illegal interception of communications in its judgment STS 367/2001, of 22 March. In this judgment, the Supreme Court stated: "The defence of national security cannot be used as an extra-legal reason to prevail upon the legal principles protected by the rule of law."

According to Organic Law 2/2002, the interception of communications conducted by the CNI are subject to prior judicial control. This Organic Law, which has only one article, states: "Within the development of its functions, the Director of National Intelligence shall request the competent Judge of the Supreme Court, according to the Organic Law of the Judiciary, authorisation for the adoption of measures affecting the inviolability of the home and the secrecy of communications, provided that such measures are necessary for the fulfilment of the functions assigned to the Centre. The decision shall be taken by reasoned order, which will remain secret."

---

[1] STS 1225/1995, of 1 December 1995; or STC 219/2006, of 3 July 2006.

[2] Law 11/2002, of 6 May, reguladora del Centro Nacional de Inteligencia.

[3] Organic Law 2/2002, of 6 May, reguladora del control judicial previo del Centro Nacional de Inteligencia.

No specific threshold or suspicion is set out for the decision on the interception of communications by the CNI. The judicial control is a requisite stemming directly from Article 18 Spanish Constitution (SC). The criteria the Supreme Court Judge has to take into account when granting the authorisation for the CNI to carry out interception of communications are not laid out. The statutory provisions determine that the judicial warrant shall be grounded, but as those decisions are secret, it is impossible to know what the grounds for them are. It is also unknown how many requests are filed with the Supreme Court Judge, or how many of them are granted and/or denied.

d) Customs Investigation Service

There are no powers to intercept communications in the law of criminal procedure and thus the powers are the same as regulated in the LECRIM.

3. Responsibility for the technical performance of interception measures

Within the investigation of criminal offences that fall under Article 588 LECRIM the technical performance of the interception of telecommunications is done by the judicial police, with the aid of the telecommunications service providers, when needed. This issue will be developed more extensively below.

Within the CNI, this competence lies with the officers of the CNI.

4. Legitimacy of data transfers between different security agencies

There is no precise regulation on the transfer of information from the CNI to the law enforcement agents. The provisions in the law of the CNI are very general.

Art. 4

[…]

c) To promote cooperative relations and cooperation with intelligence services of other countries or international organizations, to better fulfil its objectives.

[…]

e) Coordinate the action of different government bodies using means or procedures of encryption, ensure the safety of information technology in this field, inform on the coordinated acquisition of cryptology equipment and train their own personnel and staff from other administrations in this field to ensure the proper accomplishment of the tasks of the Centre.

According to the general rules, when the CNI detects possible elements of a criminal offence, like any other person and/or entity, theoretically it has the obligation to report to the police, the public prosecutor or the investigation judge. The general obligation to report facts related to a possible criminal offence are stated in Articles 259, 262, and 264 LECRIM. How this reporting activity is done in practice by the CNI is not public and there is no specific statutory regulation regarding it.

a) Exchange of data between law enforcement authorities and preventive police authorities

The structure and functions of the law enforcement authorities in Spain (mainly National Police and Guardia Civil) are regulated in Organic Law 2/1986, of 13 March, last modified 29 July 2015 *(Ley Orgánica Fuerzas y Cuerpos de Seguridad del Estado)*. When listing the functions, the law mentions both prevention and investigation, without differentiating which authorities or units will carry out preventive functions and which ones will carry out the investigation.

Art. 11 Functions

[…]

f) prevent the commission of criminal acts.

g) investigate crimes, discover and detain suspects, secure the instruments, effects and evidence of crime, making them available to the competent judge or court and prepare the necessary technical and expert reports.

h) detect, receive, and analyse any data of interest for public order and safety, and to study, plan, and implement methods and techniques of crime prevention.

Thus, one cannot speak of a "preventive police authority" different from the law enforcement authority. Within the organisational structure and internal division of departments those functions are more differentiated. The Royal Decree 769/1987, of 19 June on the Regulation of the judicial police, states what the specific functions of the police are when acting within a criminal investigation as judicial police, and how each of the units of judicial police is composed. But every law enforcement agent can act as judicial police when required, even if he/she is not integrated in one of the specific judicial police units.

In sum, there is no legal provision on the exchange of data between criminal investigation units and prevention or police intelligence units. This has been pointed out by scholars,[4] highlighting the need for a more precise regulation on the exact scope of activities the police can carry out within their preventive functions and how the information gathered for that aim could be transferred to the criminal investigation.

b) Passing on of data by intelligence agencies

See above, under this same paragraph.

c) Passing on of data to intelligence agencies

There is no specific regulation on this.

---

[4] See, Bachmaier Winter, "Información de inteligencia y proceso penal" in *Terrorismo, proceso penal y derechos fundamentales*, pp. 45–101.

B. Statistics on Telecommunication Interception

There is no legal provision that requires collecting statistical data on the number and type of telecommunications interceptions carried out in the criminal investigation. If such data exist, they are not public and are not available.

II. Principles of Telecommunication Interception in Constitutional and Criminal Procedural Law

A. Constitutional Safeguards of Telecommunication

The relevant constitutional provision safeguarding the right to privacy, the right to secrecy of communications, and the *habeas data* is Article 18 SC which reads as follows:

Article 18 SC

1. The right to honour, to personal and family privacy and to the own image is guaranteed.

2. The home is inviolable. No entry or search may be made without the consent of the occupant or a legal warrant, except in cases of flagrante delicto.

3. Secrecy of communications is guaranteed, particularly of postal, telegraphic and telephonic communications, except in the event of a court order to the contrary.

4. The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.

The precise scope of the concept of privacy, the secrecy of communications, and the definition of what should be considered as personal data has been established by the case law of the Constitutional Court and the Supreme Court.

The principles of proportionality and necessity are not expressly set out in the text of the SC when addressing the limits of fundamental rights. These principles were also not expressly stated in the Spanish Code of Criminal Procedure of 1882. However, despite the lack of a specific provision requiring that the principles of proportionality and necessity are to be respected when ordering and carrying out any coercive measure within the criminal investigation, these are elements that have been well elaborated by both Constitutional Court and Supreme Court in their jurisprudence, following the case law of the ECtHR on Article 8 ECHR.

Regarding the interception of communications (telephone), the Constitutional Court in its decision 49/1999, of 5 April 1999 stated that the principle of proportionality requires that both the legal provisions and the practice on telephone interceptions are limited to a constitutionally legitimate aim[5] and such interference will

[5] See SSTC 48/1995, of 14 December; 108/1986, of 29 July; 90/1983, of 7 November.

only be justified if the restrictive measure is strictly necessary to achieve that aim and such sacrifice is proportionate.

The investigation of a serious criminal offence is considered a legitimate constitutional aim, without having to be stated expressly in the Constitution. In assessing the principle of necessity, the relevant criterion is the possibility of achieving the same results through other measures less intrusive in the sphere of fundamental rights, taking into account the risks for securing the evidence and also the dangers for the law enforcement agents. In a strict sense, proportionality is understood as the relation between the encroachment on the fundamental right and the importance of the aim sought.[6]

To analyse the proportionality of telephone tapping, the Constitutional Court mentions which criteria should be taken into account: not only the seriousness of the crime and the penalty foreseen for it, but also other elements like the legal values protected and the social relevance of those legal values, the degree of suspicion, and the possibility to obtain the evidence by other less intrusive means.

In general, it can be stated that the Spanish courts have strictly followed the parameters set out in the case law of the ECtHR.[7]

However, Spain has in the past had problems in complying with Articles 6 and 8 of the ECHR and has several times been found in violation of the ECHR for lack of enough legal foreseeability as to telephone interceptions.[8]

Finally, in its inadmissibility decision *Abdulkadir Coban*, of 25 September 2006, the ECtHR considered that although the Spanish statutory rules were not sufficient to comply with the standards on legal foreseeability, the Supreme Court case law

---

[6] The principle of proportionality is not expressly mentioned in the Spanish Constitution of 1978, but Article 106.1 SC recognises it as a guiding principle of administrative law by stating: "1. The Courts control the power to issue regulations and to ensure that the rule of law prevails in administrative action, as well as to ensure that the latter is subordinated to the ends which justify it." On the constitutional doctrine regarding the principle of proportionality, see, among others, González Beilfuss, *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional*; Bernal Pulido, *El principio de proporcionalidad y los derechos fundamentales*; Pedraz Penalva and Ortega Benito, "El principio de proporcionalidad y su configuración en la jurisprudencia del Tribunal Constitucional y en literatura especializada alemana," pp. 69–100; Barnes Vázquez, "Introducción al principio de proporcionalidad en el derecho comparado y comunitario," pp. 531 ff.; Vidal Fueyo, "El principio de proporcionalidad como parámetro de constitucionalidad de la actividad del juez," pp. 427–447.

[7] See, among others, ECtHR, *Klass and Others v. Germany*, 6 September1978; *Malone v. United Kingdom*, 2 August1984; *Kruslin v. France*, 24 April 1990 and *Huvig v. France*, 28 September1995; *Kopp v. Switzerland*, 25 March1998.

[8] ECtHR, *Valenzuela Contreras v. Spain*, 30 September1998; *Prado Bugallo v. Spain*, 18 February2003 See generally on the case law of the ECtHR against Spain regarding telephone interceptions, Bachmaier Winter, "Telephone tapping in the Spanish Criminal Procedure: An Analysis from the European Court of Human Right's Perspective," *Rev. JURA*, 2007/2, Pécs, pp. 7–15.

provided enough guidance in this respect.[9] Thus, the situation until 2015 had been the following: an insufficient legal provision completed with the criteria set out in the case law of Supreme Court and Constitutional Court.[10]

Besides the lack of sufficient legal rules on duration, requirements, remedies, etc., regarding telephone interceptions until the reform of 2015, the Spanish Code of Criminal Procedure neither provided for a list of offences nor a penalty threshold where the interception of communications could be considered as proportional and thus could be ordered. In short, the statutory law did not define what the proportionality principle should be, and thus it had to be defined in each case by the courts. In general until reform of the LECRIM in 2015, the courts considered that the interception of communications could only be ordered for the investigation of crimes sanctioned with a custodial penalty of at least three years, or if lower, the interception could also be granted if the crime involved a criminal organisation.

This situation changed with the legal reform of the LECRIM of 5 October 2015, which will be reflected when addressing each of the questions below.

1. Core area of privacy

Following the case law of the Spanish Constitutional Court, the right to privacy *(intimidad)* recognised under Article 18.1 SC is linked to the sphere of life a person wants to preserve from prying eyes, that area the individual wants to keep hidden from others because it belongs to his/her private sphere (STC 151/1997, of 29 September 1997). This right is closely linked to human dignity and the right to the free human personal development (Article 10.1 SC). Thus, the right to an inaccessible core area of privacy is granted even to those persons who are most exposed to public view (STC 134/1999, of 15 July 1999). The right to privacy, according to the constitutional provision, is recognised not only with regard to the individual, but also with regard to the family (SSTC 197/1991, of 17 October 1991; or 231/1988, of 2 December 1988).

Based on this premise, the extent and scope of the right depends on the particular circumstances of the case, the type of life of the person and the specific aspect of his/her life that is affected (STC 115/2000, of 5 May 2000, SSTC 83/2002, of 22 April 2002 and 196/2004, of 15 November 2004).

---

[9] See Montón Redondo, "Las interceptaciones telefónicas constitucionalmente correctas," pp. 1043–1052; Gimeno Sendra, "Las intervenciones telefónicas en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo," pp. 1617–1624.

[10] See, e.g., the following decisions of the Spanish Constitutional Court: STC 239/1999, of 20 December 199920.12.1999; STC 126/2000, of 16 May 2000; STC 202/2001, of 15 October 2001; STC 167/2002, of 18 September 2002; STC 184/2003, of 23 October 2003; STC 205/2005, of 18 July 2005; STC 26/2006, of 30 January 2006; STC 72/2010, of 18 November 2010; or STC 145/2014, of 22 September 2014.

Within the criminal investigation, the protection of the right to privacy is always linked to the proportionality of the measure according to the judicial assessment. However, there is no sphere of privacy that is absolutely protected from being investigated within a criminal procedure (Spain has no "Tagebuch-doctrine").

2. Right to informational self-determination

In the landmark decision of the Constitutional Court 292/2000 of 30 November 2000, which decided the unconstitutionality challenge brought by the Ombudsman against several provisions of the Law on Personal Data Protection, the Spanish Constitutional Court made a clear and sharp distinction between the concepts of privacy and the protection of personal data, arguing that:

> "The peculiarity of the fundamental right to data protection, so close to that of privacy, lies in its distinct function, purpose and content, differently from the function of the fundamental right to privacy of Art. 18.1 SC which is to grant protection against any interference in the area of personal and family life by third persons (e.g., STC 144/1999, of 22 July 1999, FJ 8).
>
> The fundamental right to data protection is intended to guarantee that the individual has the power of control over their personal data, their use and destination, in order to prevent any illicit and damaging transfer of those data that may affect the dignity and the rights of the affected person."

In short, the judgment of the Constitutional Court stated that the right to privacy aims to guarantee the individual an area of privacy, where the interference of third persons is excluded, whilst the right to informational self-determination recognises a power of control over the information regarding him/herself, about its use and destination, to avoid an illicit use of it.

It is important to add that the fundamental right to privacy does not provide by itself sufficient protection for the new situation arising from technological progress and therefore, with the constitutional provision of Article 18 paragraph 4 SC, the right to *habeas data* and informational self-determination is granted specific protection.

3. Proportionality of access to data

In general, proportionality is a prerequisite that has to be met for the constitutional validity of any investigative measure restrictive of fundamental rights, thus also regarding access to data.

Unlike in other constitutions, the SC does not explicitly mention nor regulate the principle of proportionality as a guiding principle or parameter for the actions of public authorities. The Constitutional Court has based the application of the principle of proportionality on different Articles: the rule of law clause (Article 1.1 SC), justice as a higher value (Article 1.1 SC), or the prohibition of arbitrariness (Article 9.3 SC), although, e.g., the STC 160/1987, of 27 October established a link be-

tween the proportionality principle and the dignity of the person (Article 10.1 SC). The Court has also recognised that Article 10.2 SC supports the adoption by the Spanish courts of the case law of the Strasbourg Court on proportionality and reasonableness for the valid restriction of fundamental rights.

In the very relevant STC 55/1996, of 28 March the Constitutional Court stated that "the principle of proportionality in our constitutional system is not an autonomous constitutional principle which can be invoked separately from other constitutional rights. In the 90s the Spanish Constitutional Court started to fix the elements of the principle of proportionality under clear, although not explicitly recognized, German inspiration (e.g., SSTC 66/1995, 55/1996, 207/1996 and 136/1999)." Today it is established that the check of proportionality is comprised of: control of the adequacy or appropriateness of the measure under consideration (means-end relationship); an examination of the need for it (absence of a less intrusive alternative measure); and the strict proportionality control (the conflicting interests involved which are to be weighed to check if the advantages outweigh or at least offset the disadvantages).

Prior to the legal reform of LECRIM of 5 October 2015, the proportionality of the telecommunications interception, was assessed against those elements by the investigating judge competent to grant it. Generally, it has been considered that the minimum threshold for authorising communications interception should be three years, although exceptions are to be found in the case law, justified by the presence of an organised group, or economic or social relevance of the act.

The proportionality and reasonableness of the interference into the fundamental right has to be clearly set out in the judicial warrant, although in practice many of these judicial warrants are quite sparse in their motivation. Generally, the gravity of the offence (a penalty higher than three years imprisonment) and the absence of less intrusive measures to reach the same result are the grounds invoked in the judicial warrants authorising any telecommunications interception.

The interception of content data needs to be more substantiated than access to traffic data, as the latter implies a less intrusive measure in the sphere of fundamental rights.[11]

Since the legal reform of 5 October 2015 entered into force,[12] the elements to be taken into account for assessing the proportionality of the measure of telecommunications interception are set out in **Article 588*bis* a. LECRIM** paragraph 5:

> The investigative measures covered in this chapter are only deemed proportional when, taking into consideration all the circumstances of the case, the limitations of the rights and interests affected do not exceed the benefits of their adoption for the public interest

---

[11] On the control of telecommunications and the right to data protection, see, Zoco Zabala, *Nuevas tecnologías y control de las comunicaciones*, pp. 102–109.

[12] The law entered into force on 6 December 2015.

> or the interests of third parties. For the weighing of the conflicting interests, the public interest will be assessed taking into account the seriousness of the crime, its social significance or the technological sphere where it has been committed, the intensity of the existing evidence and the importance of the possible information or evidence sought by the measure restricting the right.

The new rules also establish a strict penalty threshold for the type of offences where telecommunications interception is allowed, and thus *sensu contrario*, if these requirements are not met, the measure would not be proportional, and therefore unlawful. This will be discussed in more detail below.

Not meeting the proportionality test or not justifying the grounds for considering the measure restrictive of a fundamental right in compliance with the proportionality test, will render the investigative measure in breach of the constitutional right to the secrecy of communications and thus will be void.

4. Statutory protection of personal data

Article 18.1 SC establishes the protection of the "right to honour, to personal and family privacy, and to the own image." Expressly, Article 18.4 SC, within the protection of the right to privacy, states: "The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights."

The SC was one of the first to establish the fundamental right to the protection of personal data and pursuant to the protection of this fundamental right there is a complete regulatory regime in the Spanish statutory provisions in accordance with the International and European Conventions. The general rules applicable to the protection of personal data are defined in Organic Law 3/2018, of 5 December on the Protection of Personal Data and the Safeguards of the Digital Rights,[13] but there are still numerous other provisions that regulate data protection for each area.[14] Significant efforts have been made in Europe to guarantee adequate protection of the right to personal data, mainly in Convention 108, of 28 January 1981, of the European Council on the automated processing of personal data; and the European Directive 95/46/CE of the European Parliament and Council of 24 October, on the protection of individuals with regard to the processing of personal data and on the

---

[13] This Organic Law recently passed adapts the domestic legislation to the EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. 4.5.2016, L 119/1. It derogates the previous Organic Law 15/1999, of 13 December, and also the Royal Legislative Decree 5/2018, of 27 July 2018, which adopted urgent rules to comply with the EU GDPR.

[14] See Ortí Vallejo, *Derecho a la intimidad e informática*, pp. 20 ff.

free movement of such data,[15] substituted by the Regulation (EU) 2016/679, of 27 April 2016 (EU GDPR). Applicable to the data with regard to criminal proceedings is the EU Directive 2016/680 of 27 April 2016.[16]

Spanish Organic Law 3/2018 largely follows the structure and content of the EU GDPR 2016/679.[17] Law 3/2018, following Article 2.2 EU GDPR, does not apply to the processing of personal data "by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security." Article 2 Organic Law 3/2018 also excludes from its scope of application the files affecting classified information (mainly state security material).[18]

As to the court files, **Article 2.4 Organic Law 3/2018** states:

> The processing of data carried out on the occasion of processing by the judicial bodies of the proceedings of which they are competent, as well as those data within the management of the Judicial Office, shall be governed by the provisions of Regulation (EU) 2016/679 and the present organic law, without prejudice to the applicable provisions of Organic Law 6/1985, of July 1, of the Judiciary.

Finally, according to the transitional provision 4 of the Organic Law 3/2018, the data covered by EU Directive 2016/680 of 27 April,[19] shall continue to be governed by former Organic Law 15/1999, as long as the Directive is not transposed.

For the protection of data linked to networks and communication services, the relevant statutory provision is Article 38 of the General Law on Telecommunications, which lists all the rights that assist consumers and users of telecommunications services.

---

[15] Extensively on this Directive, see generally Heredero Higueras, *La Directiva Comunitaria de proteccion de datos de carácter personal*, pp. 7 ff.

[16] EU Directive 2016/680 of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[17] Martín Casallo, "Implicaciones de la Directiva sobre protección de datos en la normativa española," pp. 75–86.

[18] On the exclusion of these data from the scope of application of the Law of 1999 on Data Protection for reasons of national security, see Serrano Pérez, *El derecho fundamental a la protección de datos. Derecho español y derecho comparado*, pp. 405 ff.

[19] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 "On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA." On the content of this Directive, see generally González Cano, "Cesión y tratamiento de datos personales, principio de disponibilidad y cooperación judicial en la Unión Europea," pp. 41–80.

a) Criminal liability for the unlawful interception of telecommunications

The criminal liability for unlawful interception of telecommunications within the criminal proceedings is provided under Article 539 Criminal Code (CC). I will mention here also the rules on unlawful interception of other communications and the unlawful entering of the home, as they may play some role when electronic data are collected.

The three provisions are enumerated under the heading "Of the offenses committed by public officials against the inviolability of the home and other privacy safeguards."

Article 534 CC

1. The authority or public officer who, within criminal proceedings, and without respecting the constitutional or legal guarantees:

1º-enters into a home without the consent of the occupant;

2º-records any papers or documents of a person or objects that are in his/her home, unless the owner has freely consented;

shall be punished with a fine of six to twelve months and disqualification from public office for two to six years.

If immediately after registration, the papers, documents and recorded effects are not returned to the owner, the penalty will be special disqualification from public office for six to twelve years and a fine of twelve to twenty-four months, independently from the penalty corresponding to the offence of misappropriation.

2. The authority or public official who, during lawful registration of papers, documents or effects of a person commits any unjust harassment or unnecessary damage to the property, shall be punished with the penalties for these facts, imposed in the upper half and also with the penalty of special disqualification from public office for a period of two to six years.

Article 535 CC

The authority or public officer, who, within criminal proceedings, intercepts any kind of private postal or telegraphic correspondence with violation of constitutional or legal guarantees, shall incur the penalty of disqualification from public employment or office for two to six years.

If the information obtained is divulged or distributed, the disqualification penalty shall be imposed in the upper half, as well as the fine from six to eighteen months.

Article 536 CC

The authority, public official or agent who, within criminal proceedings, intercepts telecommunications or uses any technical devices for eavesdropping, transmission, recording or reproduction of sound, image or any other communication signal, with violation of the constitutional or legal guarantees, shall be liable to a penalty of special disqualification from public office of two to six years.

If he/she reveals the information obtained, the disqualification penalty will be imposed in its upper half as well as the fine from six to eighteen months.

b) Protection of professional secrets in criminal procedural law

Certain professional secrets are protected in LECRIM through the privilege to refuse testimony, set out under Articles 416 and 417 LECRIM. These provisions have only partly been updated since 1881 and would need to be redrafted to provide more certainty. As for now, after the amendments introduced to paragraph 3 by Organic Law 5/2015, this provision reads as follows:[20]

Article 416 LECRIM

The following persons are exempted from the obligation to testify:

1. The relatives of the accused in direct ascending and descending lines, spouse or relationship analogous to marriage, their brothers or half blood and collateral blood relatives up to the second degree and relatives referred to in number 3 of Article 261.

The investigating judge has to warn the witnesses of the preceding paragraph that they are not obliged to testify against the accused, but can make the statements they deem appropriate.

2. The lawyer of the accused, regarding the facts that he has been entrusted with in his capacity as defender.

3. The translators and interpreters with regard to the conversations and communications between the accused and the persons mentioned in the preceding paragraph, in relation to the facts to which he was referred for translation or interpretation.[21]

Furthermore, Article 417 LECRIM states that the following persons may not be obliged to testify: 1) priests, pastors, or religious ministers, with regard to the facts entrusted to them in the exercise of their pastoral functions; 2) public officials subject to state secrecy;[22] and 3) morally or physically incapacitated persons (the expression "morally" incapacitated is to be understood as mentally disabled).

No other provisions are included in LECRIM for protecting professional secrets. Spanish procedural law is very sparse in this regard and needs to be updated to include scattered rules on professional secrets. For example, the legislation on law enforcement establishes that their members are subject to the rules on state secrets.[23] On the other hand, despite not being mentioned in the LECRIM, journalists cannot be obliged to give information or testify about their sources of information, as this professional secret is granted constitutional protection under Article 20.1 SC.

---

[20] Although paragraph 1 of Article 416 LECRIM refers to the spouse (and analogous relationship) privilege and also to the close relatives, and thus is not properly a "professional" secrecy protection, it is reproduced here for clarity reasons.

[21] This last paragraph was amended in order to adapt the Spanish legislation to the EU Directives 2010/64, of 20 October and 2012/13, of 22 May 2012.

[22] The rules on state secrets and classified information are mainly included in the Law on state secrets (Ley de Secretos Oficiales) 9/1968, of 4 April 1968, which was amended deeply by Law 48/1978, of 7 October 1978 and later also in 2002.

[23] See Article 5.5. Organic Law 2/1986, of 13 March, and Article 19 Organic Law 11/2007, of 22 October, the latter one specifically regulating the professional secrecy of the members of the *Guardia Civil*.

c) Principle of "purpose limitation of personal data"

This principle is set out in Article 16 Organic Law 3/2018, on Data Protection and Safeguards of the Digital Rights – which directly refers to Article 18 of the EU GDPR –, together with the principle of accuracy of data (Article 4), the principle of consent (Article 6), the right to access (Article 13), and the right to rectification/deletion of data (Articles 14 and 15) as well as the confidentiality of data processing (Article 5). Although the principle of purpose limitation also applies to non-automatic data processing, given the fact that information technologies enable massive collection and storage of personal data and the cross-referencing of such data special importance must be given to purpose limitation. Only data that is suitable and relevant for the purpose for which they were collected may be processed and used. Furthermore, the storing of excessive data or for an unjustified period of time is unlawful.

With regard to the personal data related to criminal investigations, crime prosecution and prevention, the principles set out under Article 4 EU Directive 2016/680 are the ones applicable.

The interconnection of national databases between public administrations basically affects the principle of consent and that of quality. Only databases that have compatible purposes may be interconnected without the consent of the data subject and those data can be processed without his/her previous consent (Article 18 GDPR). The question has been raised whether the transfer of data amongst different public agencies – e.g., the Tax Agency and Social Security Administration – without common powers or purposes may occur, as this might be necessary and useful in practice for the efficiency of the administration.[24] The Spanish Constitutional Court in the decision 292/2000, of 30 November stated that the interconnection of data amongst different public agencies for different purposes or matters is only legitimate and in accordance with the fundamental right to personal data protection if there is a specific legal provision that enables it or if the affected person expressly consents. Although the interconnection is technically feasible, in order to be lawful it must fulfil the conditions stated by the Constitutional Court.

The transfer of personal data to third countries that fall within the scope of application of Organic Law 3/2018, are subject to the conditions set out under Articles 44 to 50 of the EU GDPR. For the data covered by the EU Directive 2016/680, the provisions of the former Data Protection Organic Law 15/1999 apply, according to the transitional provision 4 of Organic Law 3/2018, in so far as they are applicable. This opens a certain margin of uncertainty regarding the exact legal provisions that are applicable to the transfer of data related to criminal investigations. Thus, the rules set out under Articles 35 to 40 of the relevant Directive should be applicable. As long as the transposition of the Directive is not completed, as a gen-

---

[24] See Troncoso Reigada, "Protection of data in e-government," p. 23.

eral rule, the consent of the data subject and the previous authorisation of the Director of the Data Protection Agency should be needed. The data transfer to a third country will be registered by the Data Protection Agency, with indication of the country in question and the causes that motivated the transfer.[25]

However, neither the authorisation of the supervising authority nor the consent of the data subject was needed under Organic Law 15/1999 in the following cases (only those affecting the criminal justice system are noted): 1) when the international transfer of personal data is allowed by an International Treaty; 2) when the transfer of personal data is done at the request of a judicial authority within the field of international judicial cooperation; 3) when the transfer of data is needed for the protection of a public interest recognised by law, e.g., for the fulfilment of the tasks of the tax and customs administration; 4) when the data transfer is addressed to a Member State of the European Union and the Commission has declared that the third country in question has adequate safeguards to protect the right to personal data;[26] 5) for the transfer of data within the SIS, according to the Schengen Agreement; and 6) for the transfer of data recorded in police databases for a specific investigation, when the request comes from Interpol or other channels established in international treaties. In these cases, the data will be transferred if it is needed for an actual criminal police investigation in a third country.[27]

d) Data protection of service providers' files and information gathered from interception of communications

The situation of data protection as regards files that have to be stored following Data Retention Law 25/2007, of 18 October[28] – clarified by Royal Decree 1720/2007 of 21 December – which approved the regulatory framework implementing the Organic Law on Data Protection (Organic Law 15/1999, of 13 December on the protection of personal data). Title VIII develops in detail the regulation

---

[25] Instruction 1/2000, 1 December of the Data Protection Agency, regarding the rules to be applied in the international transfer of personal data.

[26] Article 33 a), b), h) and k) Organic Law 15/1999.

[27] See Articles 3 and 4 Royal Decree 1332/1994, of 20 June 1994.

[28] Law 25/2007, of 18 October on data retention related to electronic communications and the public telecommunication networks. This law transposed the EU Directive 2006/24/EC on Data Retention. Although the Directive was later declared contrary to the privacy rights by the CJEU in the judgment of the Grand Chamber of 21 December 2016 (joint cases C-203/15 and C-698/15), for being contrary to Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, the Spanish legislator has so far not changed the Spanish data retention law.

of various security levels, distinguishing between files and authorised and unauthorised processing. The regulation establishes a definition of the level of protection required for the files that are under the responsibility of telecommunication service providers, giving precise content to the requirement of guaranteeing the authenticity, confidentiality and integrity of the information obtained from the interception under Article 97 Telecommunication Law. Following the Regulation of 2007, these are the levels of protection to be ensured: Traffic data and location data undergo the basic and medium levels of protection, but the registry of accesses will be recorded according to the higher level of protection (Articles 103 and 81.4). The access log is certainly a crucial safeguard to ensure the authenticity and non-tampering of the different information stored by order of the data retention law.

The remaining data, in particular identification data of the user or subscriber, is subject to the basic level of protection as long as it does not allow a user profile to be created, in which case it would also be subject to the middle level of protection (Article 81.1 and 2 f).

The fourth paragraph of Article 81 paragraph b) states that the information provided to the authorised agent who carried out the interception of communications will be subject to the higher level of data protection. This higher level protection ensures a level of transparency in the management and the non-manipulation of the data obtained, dispelling doubts about the integrity of the evidence, and at the same time allowing the parties to test whether communications and data submitted by the operators concerned have been subject to manipulation or unauthorised access, and, if so, to what level.

e) Rules on cancelling data stored in police files

According to the Resolution of 30 June 1995 issued by the General Directorate of the Police, a distinction must be made between three different categories of police activities:

a) Police actions carried out within state security or within the fight against serious forms of organised crime (terrorism, drug-trafficking money laundering, and all other criminal acts committed by organised groups). These data are not subject to the application of the safeguards and requirements established in the Organic Law for Data Protection.

b) Police actions aimed at the prevention of other real dangers not included in the previous paragraph. The personal data obtained within these investigations shall be cancelled by the police within 5 years of the moment the last data were added.

c) The police actions developed in the field of criminal repression and investigation which have required the use and storage of personal data will be cancelled within five years of when the criminal proceedings ended with a conviction. The time limit will start to run the moment the penalty is enforced.

B. Powers in the Code of Criminal Procedure

1. Requirement of (reasonable) clarity for powers in the law of criminal procedure

When it comes to the division of powers between the different actors that intervene in criminal procedure, there is no comprehensive regulation of all the investigative measures that can be adopted by the police, but rather a general rule of the powers of the judicial police within the criminal investigation.

The lack of a complete regulation of the powers of the judicial police in LECRIM is due to the idea underlying the whole structure of criminal proceedings in LECRIM: the investigating judge *(juez de instrucción)* directs the criminal investigation and gives precise instructions to the judicial police officers. Although this division of functions is no longer completely true in every case, the statutory rules still conform to that model. Generally, the police may carry out all the necessary investigative acts to find out the circumstances of the offence and the author or persons involved in it, except those measures that need a previous judicial warrant (Article 549.1 a) LOPJ and Article 282 LECRIM). Specifically, the Judicial Police Act (Royal Decree 769/1987, of 19 June 1987) states that, at the crime scene, the police shall observe the scene, try to reconstruct the facts and collect all elements that could be used as evidence or that could help identify the offenders. To find out the identity of the offenders, the police may perform DNA analysis, expert studies of voices, show photographs of possible perpetrators to the victims and the witnesses and line-up identifications. They can make inquiries to find out where the suspects can be found and interrogate witnesses. The police are also empowered to carry out alcoholic tests and drug controls on drivers, regardless of whether or not there has been an accident with possible criminal consequences. Furthermore, they have to adopt those measures necessary to protect the victims and detain the suspect or suspects, if possible.

Police cannot adopt any measure that restricts fundamental rights without a previous judicial warrant, except the entering of a domicile when the action is urgent (Article 553 LECRIM).

The term “coercive measure” is not defined in LECRIM and it is not usually a concept that is used by scholars or courts. The usual classification distinguishes between “measures restrictive of fundamental rights” and the rest.

Although a majority of investigative methods interfere in some way with the fundamental rights of the person under investigation or even third persons, in LECRIM only those measures which are subject to a judicial authorisation fall within the category of “measure restrictive of fundamental rights.” These are precisely: search of dwellings, interception of communications (direct, postal, telecommunications – telephone, internet, or others –), body searches other than external and the investigation by an undercover agent. The controlled delivery of drugs

requires a judicial warrant, but this measure may also be adopted by the head of the relevant judicial police unit. In LECRIM there are no provisions concerning other investigative measures carried out by the police, like cross-referencing data or other kinds of surveillance, and thus the prerequisites to adopt these measures, which undoubtedly can interfere with the fundamental rights of citizens, are not clearly defined.

The public prosecutor may direct preliminary pre-trial police investigations in certain criminal proceedings before the case is handed over to the investigating judge.[29] According to LECRIM, the pre-trial stage is directed by the investigating judge under the direct supervision of the public prosecutor (Article 302 LECRIM). This has been the distribution of functions since LECRIM was enacted in 1882. However, since 1988 in the so-called "abbreviated proceedings" (proceedings for offences sanctioned with a penalty of up to nine years imprisonment, thus the majority of cases), the preliminary investigation may be carried out by the public prosecutor (Article 773 LECRIM), before the judicial inquiry is started. The only investigative acts the public prosecutor cannot order are those measures "restrictive of fundamental rights," as stated above.

2. Differentiation and classification of powers in the law of criminal procedure

See answer under 1.

III. Powers for Accessing Telecommunication Data in the Law of Criminal Procedure

A. Overview

Since 6 December 2015 (the date the reform of LECRIM by Organic Law 13/2015 entered into force), Article 588 LECRIM allows telecommunications interception within the criminal procedure under the conditions and requirements explained below.

For the interception of communications by the CNI, the Organic Law 2/2002, of 6 May – which only provides for the requirement of judicial control of the interception of communications by the CNI –, is still applicable.

---

[29] On the investigative powers of the Spanish public prosecutor during the pre-trial stage of the criminal proceedings, see Aguilera Morales, *Las diligencias de investigación fiscal*, p. 141 ff.

B. Interception of Content Data

1. Statutory provision

Until Law 13/2015, of 5 October 2015, Article 579 LECRIM was the only provision regulating – in a very incomplete form – postal, telegraphic, and telephone communications interceptions.

If we focus on telephone interceptions, the regulation on telephone tapping was introduced quite late in the statutory provisions of LECRIM, mainly due to the judgments of the ECtHR against Spain, stating that the lack of a specific regulation constituted a violation of Article 8 ECHR. As a consequence of the case law of the ECtHR, the law was changed to meet the ECHR requirements of "legal basis," but unfortunately in a very incomplete manner. Article 579.2 LECRIM, as reformed in 1988, stated that "a court may also authorise, in a reasoned decision, the monitoring of the telephone calls of a person charged if there is evidence to show that facts or circumstances material to the case may thereby be uncovered or verified". This legal provision still did not comply with the requisite foreseeability standard, as declared in the cases *Prado Bugallo v. Spain*, of 18 February 2003 and *Valenzuela Contreras v. Spain*, of 30 July 1998. The *Naseiro* case before the Spanish Supreme Court (Decision (auto) of 8 June 1992) was the first judicial decision where the Spanish Supreme Court defined precisely and comprehensively the conditions that telephone interception must comply with. After this Supreme Court decision, the Constitutional Court rendered a judgment (STC 49/1999, of 5 April 1999), stating in full detail the legal and constitutional requirements telephone tapping should meet in order to be lawful. As had been explicitly recognised by the ECtHR in its decision *Abdulkadir Coban* already cited, the legislative reform of 1988, together with the well-established case law of the Spanish courts since 1992, constituted a body of law on telephone tapping that was adequate to provide a sufficient legal basis for the interception of telephone communications in Spain.

In addition to having a sufficient legal basis, according to Spanish law, interception of telephone communications must meet the following requisites to be justified: the aim pursued must be consistent with the Constitution; the measure must be adequate to achieve the goal pursued, i.e., to obtain data of substantial value that will elucidate the investigation of the crime at issue; it must be necessary, thus phone tapping has to be excluded if there is a different means to achieve the aim pursued; there must be a reasonable balance between the fundamental right at stake and the expected result that the measure should obtain. The Constitutional Court has affirmed that the proportionality of the measure must be considered "through an analysis of the circumstances existing at the time it was accorded," STC 126/2000, of 16 May 2000.

The Spanish system, however, was still lacking a specific and complete regulation on the interception of electronic communications. Such measures were adopted

by resorting to the rules provided for telephone tapping, rules that were not always apt to meet the needs of other telecommunications interceptions. Since the 90s scholars and practitioners have been requesting an adequate and comprehensive legal regulation of telecommunications interceptions.[30]

The insufficient regulation in LECRIM was to be interpreted and complemented with the regulation of Article 33 paragraphs 1 and 2, of Law 32/2003, of Telecommunications *(Ley General de Telecomunicaciones)*, of 3 November 2003 (BOE No. 264 of 4 January 2003), as amended by the final provision of Law 25/2007, of 18 October, on Retention of Data Relating to Electronic Communications (BOE No. 251 of 19 October 2007), which recalled expressly that the restriction of the secrecy of electronic communications was in accordance with Article 18.3 Constitution and the organic laws developing its content.

Complete regulation has recently been provided by the legal amendment of LECRIM of 5 October 2015. The next subchapter will refer to the new regulation.

The main legal provision for telecommunications interception within criminal proceedings is the new lengthy Article 588 LECRIM, which covers all possible interceptions of communications: telephone and electronic communications (Article 588*ter* LECRIM); eavesdropping or interception of oral communications and recording of images through hidden devices (Article 588*quater* LECRIM); the use of technical devices for surveillance and geo-location (Article 588*quinquies* LECRIM); the search of massive information storage devices (Article 588*sexies*); and the remote search of computers and computer systems (Article 588*septies*).

Within this paragraph, only the interception of telephone or electronic telecommunications (content) are dealt with. The general provisions are set out under Article 588*bis* LECRIM.

The general guiding principles under **Article 588*bis* LECRIM** state:

1. During the investigation of the criminal case, investigative measures covered by this chapter may be adopted provided that there is a judicial warrant issued with full respect for the principles of specialty, adequacy, exceptionality, necessity and proportionality of the measure.
2. The principle of specialty requires that a measure is related to the investigation of a specific offense. No IT investigative measure shall be authorized which aims at preventing or discovering a crime where there are no clear factual suspicions.
3. The principle of adequacy will define the objective and subjective scope of the measure as well as its duration, taking into account the usefulness of the measure.
4. In applying the principles of exceptionality and necessity, the IT investigative measure shall only be granted:

---

[30] See, among others, Montón Redondo, "Las interceptaciones telefónicas constitucionalmente correctas," pp. 1043–1052; Gimeno Sendra, "Las intervenciones telefónicas en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo," pp. 1617–1624.

a) when less restrictive measures for the fundamental rights of the investigated or prosecuted person which are equally useful to clarify the facts are not available, in view of their characteristics, or

b) when the discovery or verification of the investigated fact, the determination of its author, the investigation of his whereabouts or the location of the effects of the crime would be severely hampered without resorting to this measure.

5. The investigative measures covered in this chapter are only deemed proportional when, taking into consideration all the circumstances of the case, the limitations of the rights and interests affected do not exceed the benefits of their adoption for the public interest or the interests of third parties. For the weighing of the conflicting interests, the public interest will be assessed taking into account the seriousness of the crime, its social significance or the technological sphere where it has been committed, the intensity of the existing evidence and the importance of the possible information or evidence sought by the measure restricting the right.

2. Scope of application

a) Object of interception

LECRIM uses the heading "Interception of telephone and electronic communications" *(Interceptación de las comunicaciones telefónicas y telemáticas)*. **Article 588*ter* b. LECRIM** defines the scope, including also some definitions. It is worth reproducing the provision here:

1. The terminals or means of communication that can be intercepted must be those regularly or occasionally used by the investigated person.

2. The judicial warrant may authorize the access to content data and to electronic traffic data or data related to the electronic communication process, as well as those generated independently of the establishment of a particular communication, in which the person investigated is either sender or recipient, and may affect the terminals or means of communication the investigated person is owner or user of.

Interception of terminals or means of the victim can also be authorized when there is a serious risk to his/her life or integrity.

For the purposes of this Article, electronic traffic data or related data shall mean all those data that are generated as a result of conducting a communication through an electronic communications network, its making available to the user, as well as the provision of a service of the information society or a telematic communication of similar nature.

As to the interception of communications, Article 588*ter* b. LECRIM covers all electronic communications data: during transmission or data stored before, after or during the process of communication, although it does not specifically distinguish the moment at which electronic communications can be intercepted.

As to stored traffic data, there is a specific provision regulating its access under Article 588*ter* j. LECRIM that will be explained later when discussing traffic data.

b) Current matters of dispute

The debates that took place during the past decades caused by the lack of legal regulation of telephone and other telecommunications interceptions have lost much significance now that a specific provision has been adopted. There are still voices that criticise the extension of investigative powers within a criminal investigation, highlighting the risks of possible infringements of the right to privacy, or questioning the necessity of such measures for combatting criminality.[31] These criticisms are focused mainly on the measure of eavesdropping and remote search of computers, but not so much on the interception of electronic communications, where the new regulation is generally welcomed,[32] as it provides legal certainty and clear limits and safeguards.

3. Special protection of confidential communication content

a) Privileged communication

Organic Law 13/2015, of 4 October, amending LECRIM provides specific protection to communications between the defendant or suspect and his/her defence lawyer. Such communications were already protected under the case law of the Supreme Court and the Constitutional Court on the basis of the constitutional right to defence envisaged in Article 24 SC. No communication between lawyer and client can be intercepted, save the exception made by the penitentiary rules.

Chapter VIII of Title II of the General Penitentiary Organic Law 1/1979, of 26 September regulates communications and visits in the prison system. Specifically, Article 51.2, concerning the right of communication of inmates, without specifying their status as remand prisoners or convicts, reads as follows: "2. Communications of prison inmates with the defence attorney, the duty appointed attorney for the precise criminal case, or the court representatives *(procuradores)*, will be held in appropriate rooms and may not be suspended or intercepted except by judicial order and in cases of terrorism."

The conditions for these exceptional interceptions are cumulative: a judicial order is needed and such authorisation can only be granted in cases of terrorism, for preventive reasons and for avoiding destroying of evidence. The well-known case of Judge Garzón, dismissed from his judicial career as a disciplinary measure for authorising the interception of communications of an inmate and his lawyer in a

---

[31] See Bachmaier Winter, "Remote search of computers under the new Spanish Law of 2015: proportionality principle and the protection of privacy," pp. 1–27.

[32] See, e.g., Marchena Gómez/González-Cuéllar, *La reforma de la Ley de Enjuiciamiento Criminal de 2015*, pp. 10 ff.

case of corruption, makes clear the seriousness with which infringements of these fundamental rights are treated.[33]

The amendment of LECRIM of 5 October 2015 gives statutory regulation to the protection of communications between lawyer and defendant. **Article 118.4 LECRIM** introduced the following provision:

> All communications between the suspect or defendant and his lawyer are confidential.
>
> If these conversations or communications has been captured or intervened during the execution of some of the measures regulated by this law, the court shall order the removal of the recording or delivery to the recipient of the detained correspondence, noting this circumstance in the proceedings.
>
> The provisions in the first subparagraph shall not apply when there is objective evidence of the participation of the counsel in the offence investigated or his involvement together with the suspect or defendant in the commission of another criminal offense, notwithstanding the provisions of the Penitentiary Law.

The responsibility for ensuring the special protection of communications between defendant and defence lawyer lies with the investigating judge.

No other professional secrets are expressly protected from being intercepted within LECRIM, which has long been criticised by legal scholars. However, the protection of other professional secrets needs to be balanced by the investigating judge when deciding on the authorisation to intercept communications that may affect professional secrecy and confidential relationships.

If it is clear that the judge will not authorise the interception of communications between the defendant and his/her lawyer (as this would constitute an offence of rendering willingly an illicit decision, which is sanctioned under Article 447 Criminal Code),[34] then in practice it may occur, and occurs quite often, that conversations between defendant and lawyer are intercepted. The legal framework does not clearly state how to proceed in these cases. If the conversations are in another language or the interlocutors do not identify themselves, it may not be possible to know at the moment of recording of the conversation that the privileged lawyer-client relationship is being affected. In such cases, the interception will continue and the critical conversations shall be deleted by the investigating judge. This is, however, not specifically provided for in LECRIM.

---

[33] See the comprehensive study of Manso Porto, "Las escuchas telefónicas entre abogado defensor y cliente en una comparación internacional," pp. 39–95, in particular, pp. 64 ff.

[34] According to Article 447 Criminal Code, judges shall be held criminally liable for criminal offences committed in the exercise of their functions. In particular, knowingly passing an unjust judgment constitutes a criminal offence. The penalty varies, depending on whether the judgment has been rendered in a criminal procedure or not, and if the penalty has been executed or not. The penalty ranges from six months to four years imprisonment or a fine. In all cases, this criminal offence will entail the dismissal of the judge and the prohibition to exercise any public post for up to a maximum of 20 years.

There is no legal provision that states that the police shall suspend immediately the recording of a communication when it appears that the client-lawyer privilege is being infringed.

The only clear rules are: such communications cannot be authorised and cannot be used as evidence. But precise instructions as to how to proceed when such conversations are recorded by chance are not established by law. It has been expressly highlighted that the Spanish legal framework should regulate these situations and provide for clear action to ensure a stronger guarantee of the lawyer-client confidentiality.[35]

4. Execution of telecommunication interception

a) Execution by the authorities with or without the help of third parties

The execution of the interception of telecommunications will be carried out by the authorised officer of the judicial police, through the comprehensive system for intercepting electronic communications (SITEL, *Sistema integrado de interceptación legal de las telecomunicaciones*).

SITEL is an advanced software application that allows the interception not only of conversations but also of the data package that accompanies it, which is called "information associated to the communication." Thus, the geographical location of the caller or the type of contract of the subscriber is also made available by SITEL. Royal Decree 424/2005, approving the Regulation on conditions for the provision of electronic communications services, universal service and protection of users (BOE No. 102, of 20 April 2005) authorised the advanced technical process of interception of communications or SITEL to be installed on suppliers of telecommunications network services (ISP). Its functioning has not been without controversy as it allows all types of data regarding the communication to be accessed directly.[36]

The "spyware" is integrated into the networks of telecom operators, whether fixed or mobile. However, the system is only activated when there is a judicial authorisation. Upon receipt of the judicial warrant, the system sends – via a secured connection – the intercepted communication "point to point" to a central computer at the Directorate General of Police and Civil Guard, which in turn distributes it to peripheral terminals.

Only expressly authorised agents can access SITEL. To ensure full confidentiality and secrecy of the intercepted communications, SITEL has specific computers in

---

[35] Bachmaier Winter, "Intervenciones telefónicas y derechos de terceros en el proceso penal. La necesidad de una regulación legal del secreto profesional y de otras relaciones de confianza," pp. 41–82.

[36] Rodríguez Laínz, "Consideraciones jurídicas en torno a la licitud constitucional de SITEL," pp. 1–29.

police investigation units connected in a "sealed" way to the central SITEL server. The system works only "online" and no copies can be made of the intercepted material. Agents have to use special passwords and only have access to information related to the case under investigation. Only agents of the unit responsible for the relevant investigation can have access to the system.

SITEL is based on the Telecommunications Act of 2007, which established the requirements and legal prerequisites for applying and executing the interception of telecommunications, and is further developed in Regulation 425/2005, of 15 April.

b) Accompanying powers for the execution of interception

Clandestine access to houses to place equipment to record conversations held in them is now allowed under Article 588*quater* a. LECRIM. Clandestine recording of direct conversations is authorised in any public or private space, however clandestine recording of images can, as a rule, only be carried out in public spaces (Article 588*quinquies* LECRIM).

The use of a false identity or "digital undercover" activities are also provided for in the newly amended Article 282*bis* LECRIM upon judicial authorisation if this is needed for the discovery and/or investigation of a cybercrime or a crime committed by way of the internet (Article 588*ter* a. LECRIM).

The use of spyware for conducting remote computer searches is explained below. It is unclear whether it shall be considered as an accompanying power for the execution of the interception or a special mode of executing the specific measure of remote computer search.

5. Duties of telecommunication service providers to cooperate

a) Possible addressees of duties of cooperation

The duty to cooperate is established in a very broad way, as according to the law the addressees are "all telecommunication service providers and any kind of person that plays a role in facilitating the communications. No differentiation is made between cloud-providers and others" (Article 588*ter* e. LECRIM).

This provision states that all telecommunications service providers and persons involved in the process of facilitating communications, are obliged to cooperate with and assist in the execution of a measure of telecommunications interception, including the judge, public prosecutor and the member of the judicial police named in the judicial warrant.

Paragraphs 2 and 3 of **Article 588*ter* e. LECRIM** read:

> 2. The persons requested to provide cooperation will be required to maintain secrecy about the activities they were asked to perform by the authorities.

3. Those who fail to fulfil the above duties may incur criminal liability for disobedience to a judicial order.

This provision of LECRIM reproduces almost exactly Article 85 R.D. 424/2005, of 15 April, on the Regulation of the conditions for the provision of electronic communications services, universal service and user protection.

b) Content of duties to cooperate

The duties of telecommunications service providers and others involved in the communication process to cooperate are also very broadly drafted: they are obliged to provide "assistance and cooperation necessary to execute the judicial order of interception of telecommunications" (Article 588*ter* e. LECRIM). Not complying with this obligation constitutes an infringement of a judicial order, which can entail criminal liability. The offence of "disobedience" to the public authority applies also to deliberate non-compliance with a court order and is sanctioned with a custodial penalty from 3 months to 1 year and fine from 6 to 18 months (Article 556.1 Criminal Code, as amended by Organic Law, of 1 July 2015).

The service providers shall facilitate the access to all telecommunications data requested in the judicial warrant. The access shall cover all types of communications, also future communications. In urgent cases, this access shall be provided as soon as possible. Otherwise, access shall be ensured within one day since the issuing of the order, starting from 12:00 a.m.

R.D. 424/2005 expressly says that service providers are only obliged to cooperate in providing access to communications according to LECRIM and Organic Law 2/2002 on the National Centre of Intelligence.

According to **Article 88 R.D. 424/2005**, of 15 April, those data they are obliged to provide if requested in the judicial order are:

1. The service providers obliged shall provide to the authorized agent, unless that due to the service characteristics they are not available, those data included in the following list and authorized in the judicial warrant granting the interception:
   a) Identity or identities-in the sense defined in Article 84.i) – of the persons subject to the measure of interception.
   b) Identity or identities-in the sense defined in Article 84.i) – of other parties involved in the electronic communication.
   c) Basic services used.
   d) Supplementary services used.
   e) Address of communication.
   f) Signal of response.
   g) Cause of termination.
   h) Duration.
   i) Location Information.
   j) Information exchanged through the control channel.

2. In addition to information concerning the interception under the preceding paragraph, entities shall provide the authorized agent –unless that due to the characteristics of the service they are not available– the following data of any party involved in the communication that are clients of the obligated party:

a) Identification of the natural or legal person.

b) Address where the provider performs notifications.

And, even if they are not clients, if the service allows to access to the following data:

c) Number of service holder (both the directory number as all identifications of electronic communications subscriber).

d) Identification number of the terminal.

e) Account number assigned by the ISP.

f) E-mail address.

3. Along with the information specified in the preceding paragraphs, the service providers obliged shall provide, unless that the characteristics of the service does not allow it, information on the geographical location of the originating and terminating end points. In case of mobile services, it will provide the most accurate position possible to the point of communication and, in any case, the identification, location and type of the affected base station.

c) Duties to provide technical and organisational infrastructure

R.D. 425/2005, of 15 April sets out the obligation of service providers to adopt all technical measures to facilitate access to all kinds of communications (Articles 86 and 87.2), and to adopt technical measures to safeguard the right to secrecy of the communications (Article 91). The service provider obliged to cooperate shall ensure that only the authorised person is given access to communications (Article 92) and this authorised agent only has access to the communications identified in the judicial warrant, excluding any others (Article 87). The service providers shall keep the process confidential (Article 93).

d) Security requirements for data transfers by communication service providers

Article 91 R.D. 424/2005, of 15 April states that all the technical measures to ensure the safety and the secrecy of communications, as well as the confidentiality of interceptions, shall be adopted.

In case of particular security threats or breaches of the network security the Ministry of Interior and the clients shall be informed.

e) Checks, filtering, and decryption obligations of communication service providers

These issues are not specifically regulated. The general rule is that service providers are obliged to follow the instructions given in the judicial warrant granting

the interception of the communication or the access to the data. How this is done in practice is unknown to this author.

6. Formal prerequisites of interception orders

a) Competent authorities

The competence to request the measure lies with the public prosecutor and the judicial police, but it can also be ordered *ex officio* by the investigating judge (Article 558*bis* b. 1 LECRIM).

The competence to authorise telecommunications interception lies with the investigating judge (Articles 588*bis* b., 588*bis* c., 588*ter* d. LECRIM); exceptionally, in urgent cases, within the investigation of offences related to organised groups or terrorism and where there are reasonable grounds to consider the measure to be indispensable, the interception of the telecommunications can be ordered by the Ministry of Interior or, in his/her absence, by the Secretary of State for Security (immediate level below the Ministry of Interior).

The adoption of this measure shall be immediately notified to the competent investigating judge within a maximum time period of 24 hours, expressing the reasons for its adoption, the acts undertaken, and the results obtained. The judge will grant or reject the adoption of the measure in a reasoned decision within a maximum time of 72 hours since it was adopted (Article 588*ter* d. 3 LECRIM).

b) Formal requirements for applications

Requirements for the judicial application for all measures under Chapter IV, Title VIII, Book II LECRIM (interception of telecommunications, interception of direct conversations, recording of images, use of geo-location devices, computer searches and remote searches of computers and computer networks) are:

Art. 588*bis* b. 2 LECRIM

2. When the public prosecutor or the judicial police request the judge an IT investigative measure *(medida de investigación tecnológica)*, the request shall contain:

1. The description of the facts under investigation and the identity of the subject or otherwise affected person by the measure, provided that such data are known.
2. The detailed statement of the reasons justifying the necessity of the measure according to the guiding principles set out in Article 588 bis, as well as indications of the offence that have been found during the investigation prior to the application for authorization for the restrictive measure.
3. Identification data of the suspect or defendant under investigation and, if appropriate, the means of communication used by him that will allow the execution of the measure.
4. The extension of the measure specifying its content.
5. The investigative unit of the judicial police who will take over the interception.
6. The form of execution of the measure.

7. The duration of the measure sought.
8. The precise person obliged to execute the measure, if known.

For the measure of interception of telecommunications, the additional requirements of the application are set out under:

Art. 588*ter* d. LECRIM

1. The request for authorization must contain, in addition to the requirements referred to in Article 588*bis* b., the following:
   a) Identification of the number of subscriber, the terminal or the technical label,
   b) Identification of the connection which is subject of the interception, or
   c) Data necessary to identify the means of telecommunication to be intercepted.

2. To determine the scope of the measure, the application for judicial authorization may concern one of the following objectives:
   a) The registration and recording of the content of the communication, specifying the form or type of communications that are involved.
   b) The data of origin or destination of the communication at the moment in which communication is taking place.
   c) The geographical location of the origin or destination of the communication.
   d) Other related traffic data linked or not, that may add value to the communication. In this case, the request shall specify the specific data to be obtained.

c) Formal requirements for orders

The judicial warrant, according to new Article 588*bis* c. LECRIM shall be issued within a maximum time of 24 hours after the request is filed, and shall have at least the following content:

Art. 588*bis* c. 3 LECRIM

a) The punishable acts under investigation and their legal qualification, stating the reasonable suspicion to ground the measure.
b) The identity of the suspects/defendants and any other third person affected by the measure, if known.
c) The scope of the restrictive measure, specifying the extension and the compliance with the guiding principles established in Article 588*bis*.
d) The judicial police investigative unit that will take over the interception.
e) The duration of the measure.
f) The manner and frequency in which the requesting authority shall inform the judge about the results of the measure.
g) The aims sought by the measure.
h) The person obliged to execute the measure, if known, expressly stating his/her duty to cooperate and to keep the acts secret, where appropriate, being liable for the offence of disobedience of a court order.

7. Substantive prerequisites of interception orders

a) Degree of suspicion

Mere suspicion, conjecture or guesses are not enough to order the interception of telecommunications. Spanish doctrine and jurisprudence do not differentiate clearly between "sufficient or justified grounds," "reasonable suspicion," and "probable cause" to qualify degrees of suspicion. The courts and the law use the term "sufficient indications of the existence of the criminal offence." What this means in practice is not easy to define, but has been considered to be "facts that rationally – objectively assessed – indicate the probability that some person is involved in a criminal act."[37]

The Spanish case law, interpreting previous Article 579 LECRIM on telephone tapping, has repeatedly stated that evidence must consist of external data accessible to third parties that provides a real basis from which it is possible to infer that a crime has been or is about to be committed; the mere appraisal of the behaviour or the quality of a person is not admissible.[38] The initial circumstantial evidence must refer to precise criminal facts and specific persons and must be grounded on objective data. In addition, this circumstantial evidence must lead to the establishment of a connection between the people using the telephones to be intercepted and the criminal facts that are being investigated. These requirements are aimed at preventing the judge from issuing a warrant for phone tapping for the mere purpose of an exploratory search, without being linked to a concrete criminal fact.[39]

Moreover, the Supreme Court case law states that "the mere affirmation by the police of the existence of certain suspicions is not enough to order the interception of the communications" (Supreme Court Decision *(auto)* 18 June 1992, which is one of the landmark decisions), but precise facts and the origins of the information about those acts that form the basis of suspicion have to be substantiated for ordering the telecommunications interception. Anonymous information or information coming from a confidential source has usually been considered insufficient grounds for telecommunications interception.

---

[37] On the reasonable suspicion required for granting the interception of communications, see, e.g., the following judgments of the Constitutional Court, SSTC 136/2006, of 8 May 2006; 220/2006, of 3 July 2006; 219/2009, of 21 December 2009 or 26/2010, of 27 April 2010. See also Zoco Zabala, *Nuevas tecnologías y control de las comunicaciones*, pp. 208–217.

[38] STS of 11 November1996or STS of 10 October1998. See also the Constitutional Court's decision STC 184/2003, of 23 October 2003, § 11, in which the Court held that it was unconstitutional to issue a warrant of phone tapping on the exclusive basis of an anonymous denunciation of a possible crime of corruption.

[39] In the judgment 165/2005, of 20 June 2005, the Constitutional Court stated that the fact that a person did not have a job, but spent great sums of money, was not sufficient grounds to issue a warrant, as this is not an objective fact that defines the necessity of the phone tapping. More recently see STS 279/2017, of 19 April 2017.

In practice, for obtaining a judicial order authorising telephone interception, police undertake surveillance activities to gather enough information to meet the standards of "probable cause."

The question has recently been raised in some Supreme Court judgments whether the information obtained from cooperation with foreign law enforcement or intelligence services (e.g., FBI or DEA) may be enough to meet the required degree of suspicion for authorising telephone interception.

One such case relates to telecommunications interception and confiscation of a significant amount of drugs based on information provided by the US Drugs Enforcement Agency (DEA). The defence lawyer contended that the telecommunications interceptions were unlawful, as the initial suspicion was not established by lawful means. The answer of the Supreme Court was that it cannot be presumed that the sources of information of the police are unlawful, and that since in the instant case there were no indications that the information came from an illegal interception of communications, their validity was presumed, and the evidence so obtained was considered admissible (STS 884/2012, of 8 November).

Another interesting case relates to the information obtained through the interception of communications ordered by the Spanish judicial authority in execution of a letter rogatory issued by the Italian Prosecution Service of Bologna (Italy). The defence claimed that the letter rogatory was not backed with a lawful judicial authorisation and therefore the interception carried out in Spain should be considered illegal and consequently all the derived evidence from the unlawful interception should also be excluded. The Supreme Court, in the decision 475/2018, of 17 October, states that Spanish judicial authorities cannot subject the enforcement of letters rogatory to the previous scrutiny of the legality of the sources that led to the issuing of the request by the foreign authority.

b) Predicate offences

There is no closed list of offences where the measure of interception of communications can be ordered. **Article 588*ter* a. 1 LECRIM** (that refers to Article 579) lists:

1. Intentional offences punishable with a maximum imprisonment penalty of at least three years.
2. Crimes committed within a group or criminal organisation.
3. Terrorist offences.

In addition to these offences, and not subject to the minimum of three years custodial penalty, telecommunications interception can be ordered with regard to the investigation of offences committed through computers or IT equipment *(instrumentos informáticos)*, or other information technology or communication or communication services.

c) Persons and connections under surveillance

Article 588*bis* h. LECRIM provides for the possibility to authorise the investigative measures intercepting communications also when third persons are affected in the cases and under the conditions set out in the regulation of each of the measures.

Additionally, for the interception of telecommunications, **Article 588*ter* c. LECRIM** states:

> The interception of communications originating from terminals or electronic communication means belonging to a third person may be authorized, provided that:
>
> 1. there is evidence that the suspect or defendant under investigation uses them to transmit or receive information, or
> 2. the subscriber collaborates with the investigated person in their illicit acts or benefits from his activities.
>
> Such communication interceptions may also be authorized when the device which is the object of the surveillance is being used maliciously by others electronically *(por vía telemática)*, without the knowledge of its owner.

d) Principle of subsidiarity

As for any measure restrictive of fundamental rights, the interception of electronic communications must comply with the principle of subsidiarity, that is, that the same data are not reasonably accessible by less intrusive means. The assessment in each case of compliance with this requirement is to be done by the investigating authority, who in some cases will request that other means are tried first and on other occasions may accept that other means are likely to be unsuccessful. This is one of the points that requires a deep empirical analysis. Although most judges are very strict when it comes to ordering telecommunications interceptions, others just resort to a general statement that reads "considering that the data needed for the investigation cannot be acceded through other less intrusive means […]," without any further verification of whether such less intrusive means are really available or not.

e) Proportionality of interception in individual cases

The judge shall assess the proportionality of the measure in view of the seriousness of the offence to be investigated, although usually when the offence is sanctioned with more than three years custodial penalty, it is considered that it meets the proportionality principle. Usually the likelihood of obtaining the requested data is considered by the judge when ordering the interception of telecommunications. However, the likelihood does not exclude the need to comply with the requirements of necessity and proportionality.

Regarding the remote search of computers, as I have already stated, while Spanish law insists on compliance with the specificity and proportionality principles in granting and executing this investigative measure, it does not determine how these

principles are to be respected in the remote search of computers. The judicial warrant specifies whether the law enforcement authorities are authorized to copy and preserve the data and also sets out the precise measures to be carried out to preserve the integrity of the data. These are general statements that need to be concretized. The proportionality principle can be infringed at the stage of granting the access as well as when executing the measure, but nothing is stated in the law regarding the latter. It is to be defined in the judicial warrant but at present judges lack guidelines on how to proceed in this regard.[40]

On the other hand, the issue of whether a remote search of a computer is necessary in cases where the computer can be physically located and registered has not been addressed yet in Spanish practice.

f) Consent by a communication participant to the measure

Consent given by one of the interlocutors, according to the case law of the Supreme Court (STS 217/2014, of 30 January 2014), excludes the unlawfulness of the interference of the state in the right to secrecy of communications, although there are exceptions applicable within the labour law and the protection of the privacy of the employee. However, in a case where a person held in prison gave consent to the police officers to listen to his conversations, the ECtHR held that even in such a case the legal requirements for the state to intercept communications have to be followed (ECtHR *M.M. v. The Netherlands*, of 8 April 2004).

8. Validity of interception order

a) Maximum length of interception order

The general rule is that any measure restrictive of fundamental rights shall not last longer than is absolutely necessary for the discovery of the facts (Article 588*bis* e. LECRIM). For interception of telecommunications the period is three months, extendable for the same period, up to a maximum of 18 months (Article 588*ter* g. LECRIM). The whole process of execution of the measure is subject to judicial control. The judicial police shall report on the progress of the investigation within the time periods established in the judicial warrant authorising the interception of telecommunications (Articles 588*ter* f. and 588*bis* g. LECRIM). To that end, the judge may request the integral records and/or transcripts of the recorded conversations.

---

[40] See Bachmaier Winter, "Remote search of computers …," pp. 21–22.

b) Prolongation of authorisation

The duration of the measure may be prolonged through a reasoned judicial decision, by the competent judges, *ex officio* or upon application of the public prosecutor or the judicial police. The judge may prolong the measure if the reasons that justified its adoption remain (Article 588*bis* e. LECRIM). To authorise the prolongation of communications interception, the investigating judge has to check what information has been obtained and whether the need, adequacy and proportionality of the measure still exist.

If the time for which the measure was authorised expires without granting the time extension, the measure will cease. Any evidence obtained after expiry of the period, even if there is no abuse on the side of the authorities, is unlawful and will not have any evidentiary value.

The request for prolongation of communications interceptions shall be filed with enough time left before the authorisation expires. The application for an extension shall be accompanied by: 1) a detailed report on the execution of the measure and its results, and 2) the reasons that may justify the need for an extension. The judge shall decide on this application within two days (Article 588*bis* f. LECRIM). There have been numerous cases where the Constitutional Court rendered inadmissible telephone interceptions precisely because the judicial warrant granting the prolongation of the measure was not sufficiently grounded as to the reasons why the measure was still necessary.

c) Revocation of authorisation

The measure will cease once the conditions that led to its adoption disappear or it is made clear that no results are to be obtained through it, and in any event, once the timeframe has expired (Article 588*bis* j. LECRIM).

The whole execution of the communication interception is subject to regular judicial control, with a frequency established by the judge. As a consequence of this periodical control, the investigating judge may revoke the initial authorisation even if the maximum time period of three months has not elapsed. The frequency for judicial control is to be decided by each judge and will depend on the type of case. Until now, as prolongation could only be authorised for a period of one month, this was the usual frequency of judicial control of the measure.

9. Duties to record, report, and destroy

a) Duty to record and report

The reporting duties have been explained above.

As to recording, **Article 588ter f. LECRIM** provides:

> The Judicial Police will make available to the judge, at intervals determined by it, the transcription of the passages considered relevant and the complete recorded communications. The police shall indicate the origin and destination of each of the communications and shall ensure, through a sealing system or advanced electronic signature or sufficiently reliable system of authentication, the authenticity and integrity of the data dumped from the host computer to the digital files in which the communications were recorded.

b) Duty to destroy

Article 588*bis* k. LECRIM provides for the destruction of records in the following way:

> 1. Once the criminal proceedings are terminated by a final ruling, the original records that are kept in the electronic and computer systems used in the execution of the measure shall be deleted and erased, upon order. A copy of those records will be kept under the custody of the court secretary (*secretario judicial*, official who has functions as court manager, acts as notary of the procedural acts, and has powers to take certain procedural decisions).
>
> 2. The preserved copies will be destroyed after five years have elapsed since the penalty was executed or when the time for the statute of limitations of the offence or the prosecution has expired or the decision to put an end or decision of acquittal is final, unless the court considers its conservation necessary.
>
> 3. The Court shall instruct the Judicial Police to put into effect the destruction referred to in the preceding paragraphs.

Some scholars have criticised this provision because it still allows the court to order the conservation of the intercepted conversations ("provided that the court does consider the conservation necessary").[41] On the other side, this provision does not establish who shall decide on the destruction and check that it has beeg done, because it is not clearly stated who is the authority responsible for storing the evidence and then controlling its destruction. On the other side, this rule may present some inconsistencies with the rules on preserving the court files and its accompanying documents if the disks are considered as documents.

10. Notification duties and remedies

a) Duty to notify persons affected by the measure

Until the amendment by Organic Law 13/2015, of 5 October 2015, there was no legal obligation to inform third persons that had been affected by the interception of telecommunications. This was repeatedly criticised by scholars for non-compliance with the adequate protection of human rights. This flaw has been corrected with the new provision introduced recently in LECRIM, which reads:

---

[41] Oubiña Barbolla, "Datos personales y nuevas tecnologías de investigación tecnológica: oportunidades, retos y límites," pp. 276–277.

Art. 588*ter* i. 3 LECRIM

The investigating judge shall notify the persons involved in intercepted communications of the fact of the interference and shall inform them of the specific communications in which they have participated. This information shall take place unless it should require a disproportionate effort or it could prejudice future investigations. If the notified person so requests he/she will be given a copy of the recording or the transcription of such communications, insofar as this does not affect the right to privacy of others or is contrary to the objectives of the proceedings under which the measure was adopted.

This new provision stating the obligation to notify the persons whose conversations have been recorded is to be welcomed. However, as the exceptions for complying with this duty are so broadly drafted, in practice it may lead to a generalised lack of information. It has to be noted that the notification of the conversations held by a third person in most cases will "affect the privacy of others," unless the conversation was with one of the defendants.

b) Remedies

If the third person affected by the telecommunications interception should consider that there has been an unlawful infringement of his/her fundamental rights, he/she could choose to file a criminal complaint (the victim has standing to press charges in criminal cases and become, independently from the public prosecutor, a private accuser) and also claim civil damages within the criminal procedure for violation of his/her right to secrecy of communications; or file a civil suit against the relevant authority claiming damages for the infringement; or claim damages from the state for malfunctioning of the administration of justice, a procedure where guilt does not need to be proven, as there is strict liability of the state for damages caused by miscarriage of justice or malfunctioning of justice.

As the obligation to notify third parties is new and is not yet in force, there is no practice on this issue.

c) Criminal consequences of unlawful interception measures

The precise criminal sanctions provided in the Criminal Code for unlawful interceptions of communications have been explained above. As to the frequency of such infringements, it is not easy to give any accurate information. The judicial police are very much aware that any telecommunications interception is subject to a prior judicial warrant, and the strict evidentiary rule has a strong deterrent effect. Thus, there is no case law on unlawful actions of judicial police members in this regard. The main reasons for considering telecommunications interceptions unlawful, until now, have been: the lack of adequate reasoning in the judicial warrant, the lack of reasoning given for the need for prolongation, or not providing the complete recorded conversations or the whole files granting authenticity, but not for illegal acts on the part of officers. There was a case where a telephone interception

was declared void and inadmissible as evidence by the Constitutional Court because the interception had lasted some days longer than authorised in the warrant because the police had mistaken the moment from which to count the extension of 30 days.

If an officer were found to have carried out an illegal interception of the communication, he/she would not only be criminally liable for violation of the secrecy of the communications but would also be subject to disciplinary sanctions as a public servant, with possible dismissal.

As to an independent monitoring authority with power to control the interception of communications, Spain has no such body or authority. This is explained by the fact that it is considered a sufficient guarantee to subject all telecommunications interceptions to the prior judicial warrant. Since the judge is the authority that enjoys the greatest independence according to the Constitution, this is considered the best safeguard for the protection of fundamental rights.

However, the absence of any statistics or external body controlling the use that is being made in practice of the powers to intercept telecommunications does not seem to ensure sufficiently the transparency of the whole system. The fact that a measure of interception of communication can be ordered *ex officio* by the investigating judges certainly is a deficit of the system of guarantees that in my opinion should be reviewed.

11. Confidentiality requirements

Article 588*ter* e. LECRIM states that all telecommunications service providers and persons involved in the process of facilitating communications are obliged to cooperate with and assist the judge, public prosecutor and the member of the judicial police designated with the execution of the measure of telecommunications interception.

Article 588*ter* e. LECRIM paragraphs 2 and 3

2. The persons requested to provide cooperation will be required to maintain secrecy about the activities they were asked to perform by the authorities.

3. Those who fail to fulfil the above duties may incur criminal liability for disobedience to a judicial order.

Furthermore, the General Law 32/2003, of Telecommunications establishes sanctions for serious, less serious and grave infringements of the legal provisions on telecommunications services. Those sanctions are administrative fines that may rank from up to a maximum of 30,000 euros for less serious infringements to proportionate fines according to the benefit obtained (Article 56).

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

a) Collection of traffic data

Law 25/2007, of October 18 on Data Retention of Electronic Communications requires judicial authorisation to access not only traffic data (connected terminals, user identification and dating of the communication), but also other data that may be classified as value added services.

Since the reform by Law 13/2005, there is also a complete regulation of the access and transfer of traffic data by telecommunications service providers and other persons obliged to cooperate.

Article 588*ter* j. LECRIM on data contained in automated files of service providers reads:

> 1. Electronic data held by service providers or individuals that facilitate the communication in compliance with the legislation on data retention regarding electronic communications – on its own initiative or for commercial reasons or otherwise – and which are linked to the processes of communication, can only be transferred for incorporation into the procedure upon judicial authorization.
>
> 2. When knowledge of these data is indispensable for the criminal investigation, a judicial warrant shall be applied for to the aim of collecting the information contained in the computerized files of service providers, including cross-linked searches or data mining *(búsqueda entrecruzada o inteligente de datos)*. The application shall indicate which kind of data are required and what the reasons that justify the transfer of those data are.

The formal and substantive prerequisites for the collection of traffic data are the same as for content data: no specific provisions are provided in the LECRIM for filing the application for the order, nor for the content of the judicial order or the duty of telecommunications service providers to cooperate with the criminal investigation. Therefore, what has been already stated with regard to telecommunications interception of content data applies in general to traffic data. In practice, the main difference lies in the assessment of the proportionality of the measure and the required degree of suspicion to grant access to the traffic data. Although there are no precise standards or definitions in this regard, as the intrusiveness of this measure in the fundamental right to secrecy of communications and privacy is lower, courts and scientific scholarship consider that the standards for granting it could also be lowered. However, the general requisite of the type of offence and gravity of the penalty, set out in Article 588*ter* a. LECRIM (offence sanctioned with penalty higher than three years imprisonment, organised crime or terrorism, plus cybercrime offences or offences committed by using IT), applies here equally.

In fact, until now, the same general authorisation for intercepting telephone conversations was used to access all traffic and other data associated with the communication. This is possible as long as the SITEL mechanism gives access to the

whole "package" of communication data. Generally, the Supreme Court has considered that the main authorisation for content data implies also access to the traffic and associated data. However, scholars have raised the issue of the proportionality principle, as it obviously has a different impact to access only the conversations, rather than also the accompanying names, addresses and geographical location of the interlocutors.

b) Collection of subscriber data

If, in the exercise of their preventive and investigative functions regarding offences committed through the internet, judicial officers have access to an IP that is being used to commit a crime, and neither the equipment or identity of the user is identified nor is the equipment located, the officers shall request from the judge an order to obtain the identification data from the telecommunications service provider in order to identify the suspect (Article 588*ter* k. LECRIM). The requirement of the judicial warrant is based on data protection law and not on the protection of the right to secrecy of communications.[42]

In general, the identification of the subscriber of a telephone or other communication service, or otherwise the identification of the telephone number of a person, can be directly requested by the public prosecution or by the judicial police from the company providing such service (Article 588*ter* m. LECRIM).

The addressees are obliged to comply with the request, or face the penalty for the offence of disobedience. These data are provided in an automated way.

c) "Data retention"

Law 25/2007, of 18 October on Data Retention transposed into the domestic legal order EU Directive 2006/24/EU, which was later annulled. Article 3 of the Spanish law essentially reproduces Article 5 of the (annulled) Directive when listing the data that the service providers are obliged to retain. The data have to be retained for 12 months (Article 5.1 of Law 25/2007). This law is still in force and the recently enacted Organic Law 3/2018 has not derogated from it.

2. Identification of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

a) Identification of device ID with the help of IMSI-catchers

IMSI-catchers are used by law enforcement agents in their investigative activities. The Supreme Court case law has declared that the use of such devices to track the presence of mobile phones in a certain location does not need a judicial warrant as

---

[42] See recently STS 167/2018, of 2 March 2018.

such activity does not affect personal data: it only identifies the presence of an object in a certain place.[43] The same applies to IP directions (except when personal data are linked). In fact, such tracking devices and the information obtained therefrom has been used frequently in practice to underpin the judicial application for obtaining subscriber identification and later the authorisation for telecommunications interception. LECRIM does not specifically mention the use of IMSI-catchers.

It is unclear whether the new Article 588*quinquies* b. LECRIM refers to these devices or not. The heading of this provision reads: "The use of devices or technical means for tracking and location." From the heading it is unclear whether "IMSI-catchers" are included among those devices or not: on one hand they do not track a certain person, but only a mobile terminal; but on the other hand, they could fall within the category of "location devices." The content of the Article does not provide further clarity on this issue. However, it may be worth reproducing it here:

Article 588*quinquies* LECRIM

1. Where there are good reasons that show that the measure is necessary and proportionate, the judge may authorize the use of devices or technical means for tracking and tracing.

2. The authorization shall specify the technical means to be used.

3. Providers, officers and persons referred to in Article 588*ter*, are required to provide the judge, the prosecutor and the judicial police officers appointed to execute the measure the necessary assistance and collaboration to facilitate the execution of the judicial order authorizing the monitoring, under penalty of committing an offence of disobedience.

4. In urgent cases, where there are reasons to fear that if the devices are not put in place immediately, this will frustrate the investigation, the Judicial Police may proceed to their placement, informing as soon as possible and in any case within 24 hours the judge, who may ratify the measure or order its ceasing also within 24 hours. In the latter case, the information obtained from the device in place will have no effects in the criminal proceedings.

According to my interpretation, this provision is related to other tracking devices and not to IMSI-catchers. However, my interpretation cannot be seen as conclusive.

b) Location determination via "silent SMS"

LECRIM does not mention either IMSI or IMEI identification or tracking devices. Location via silent SMS is used in practice in criminal investigation, it being unclear in the case law if a judicial warrant is required for it or not. The same considerations that have been expressed above under the previous paragraph regarding the IMSI catcher are applicable here.

---

[43] Since the STS 249/2008, of 20 May 2008, the Spanish Supreme Court has admitted the use of IMSI-catchers by law enforcement. In this sense, see also SSTS 776/2008, of 18 November 2008; 406/2010, of 11 May 2010; 443/2010, of 19 May 2010; 628/2010, of 1 July 2010; 1078/2011, of 24 October 2011; or 940/2011, of 27 September 2011.

D. Access to (Temporarily) Stored Communication Data

1. Online searches with the help of remote forensic software

The new Law 13/2015, of 5 October introduces the regulation of the remote search of computer equipment. In the Spanish system, as explained above, no measures restrictive of fundamental rights can be used for preventive purposes by law enforcement. Only within the criminal procedure and with prior judicial authorisation may the new measure of remote search of computer equipment be carried out.

The new **Article 588*septies* a. LECRIM** sets out the requirements for this measure:

1. The judge may authorize the use of identification data and codes, as well as the installation of a software that allow the electronic remote search, without knowledge of the owner or user, of the contents of a computer, an electronic device, a computer system, or instruments for mass storage of computer data, or databases, for the aim of investigating one of the following offenses:
   a) Crimes committed within criminal organizations.
   b) Terrorist offenses.
   c) Crimes committed against minors or persons with legal incapacity judicially declared.
   d) Crimes against the Constitution, treason and related to national defence.
   e) Crimes committed through computer tools or other information technology or telecommunications or communication service.
2. The court order authorizing the remote search shall specify:
   a) the computers, the electronic devices, the computer systems or part of them, the data storage media or databases to be searched, and the data or other digital content targeted by the measure.
   b) The scope of it, the way in which the access and the seizure of data or computer files relevant to the case will be done, and the software by which the access and control of the information will be done.
   c) The officers authorized to execute the measure.
   d) The authorization, if any, for making and retaining copies of the computer data.
   e) The precise measures to preserve the integrity of the stored data as well as the measures for ensuring the inaccessibility or deletion of such data from the computer system that has been accessed.
3. When the officers who conduct the remote search have reasons to believe that the data sought are stored in another computer system or part of it, they will inform the judge about this matter, who may authorize an extension of the conditions of the search.

It has to be noted that the duration of this measure is much shorter than is provided for other IT investigative measures. While all other IT measures may be authorised usually for three months, extendable for equal terms up to a maximum of 18 months, the remote search of computers can only be authorised for one month, with a maximum extension up to three months (Article 588*septies* c. LECRIM).

2. Search and seizure of stored communication data

a) Special provisions

Until law 13/2005, of 5 October there was no specific regulation for the search and seizure of stored communication data, although it was used in practice under the general rules on telephone tapping (Article 579 LECRIM) or search and seizure of documents and objects. The lengthy new Article 588*sexies* a. to Article 588*sexies* c. LECRIM provides for a complete regulation of this measure, specifying the requisites for judicial authorisation, the restrictions to the seizure of computer hardware, the way to make copies of the relevant data seized and the need for a specific authorisation for this measure beyond the authorisation for searching a premises.

Article 588*sexies* a. Need for specific motivation

1. When it is foreseeable that during a domicile search the apprehension of computers, telephone or electronic communications instruments, mass storage digital information devices, or the access to telematic data repositories will take place, the judicial warrant authorizing the search of dwellings shall extend its reasoning to express the reasons, if any, that authorize the agents to access the information contained in such devices.

2. The simple seizure of any of the devices to which the preceding paragraph refers, carried out during the house search, does not authorize to access to its content, notwithstanding the possibility that such access could be authorized later by the judge.

Article 588*sexies* b. Access to information of electronic devices seized outside the home of the suspect/defendant

The requirement set out in paragraph 1 of the preceding Article shall also apply to cases in which computers, communication instruments or devices of mass data storage, and access to telematic data repositories, are seized independently from a house search. In such cases, officials shall inform the judge of the seizure of such devices. If the judge considers that the access to the information hosted in such devices is indispensible, he may grant the corresponding authorization.

Article 588*sexies* c. Judicial authorization

1. The judicial warrant authorizing access to the information contained in the devices this section refers to, shall determine the conditions and scope of the search and may authorize the copying of the computer data found. It shall also determine the conditions necessary to ensure data integrity and preservation guarantees to enable, where appropriate, the examination by an expert for preparing an expert opinion.

2. Unless they constitute the object or instrument for committing the crime or there are other reasons that justify the seizure of hardware containing computer data or files, the confiscation of the hardware will be avoided, when this would cause serious damage to the user or owner and it is possible to secure the data by obtaining a copy of them in conditions that guarantee the authenticity and integrity of the data.

An extended search of other computers connected to those placed in the domicile under search is also regulated under paragraph 3 of this Article, but it needs to be authorised specifically by the judge, if not authorised initially.

b) Different standards of protection for stored and for transmitted data

The new regulation on interception of telecommunications and access to stored data does not provide for different requisites, duration or formal requirements for real-time communications and stored communications.

What has been noted regarding the interception of content data of communications is applicable *mutatis mutandis* to access to stored electronic data. The new legal framework seems to consider stored data as communications and not documents. However, the regulation is unclear, because when regulating access to stored electronic data in computers or other electronic devices, it does not distinguish between ordinary files and stored communications.

c) Open and clandestine access to stored data

If the stored data are accessible via remote computer search (as explained below) they can also be accessed in a clandestine way, without the relevant person being aware of it. However, if the stored data are on a device or hard disk, which is not accessible via remote computer search, then in principle, the only way to access those data is by way of a search and seizure order. The execution of the home search requires the presence of the inhabitant or owner and thus it could not be carried out in a clandestine way.

3. Duties to cooperate: production and decryption orders

Art. 588*sexies*. 5 LECRIM

The authorities and officials responsible for the investigation may order any person who knows the operation of the computer system or is aware of the measures that protect the computer data, to provide the information necessary, provided that such cooperation does not entail a disproportionate burden for such person, under the penalty of committing an offence of disobedience.

This provision shall not apply to the suspect or defendant and persons who are exempted from the obligation to testify by reason of kinship and those that, in accordance with Article 416.2 LECRIM, cannot testify due to professional secrecy.

IV. Use of Electronic Communication Data in Judicial Proceedings

1. Use of electronic communication data in the law of criminal procedure

For the telecommunications interception to be assessed as evidence in criminal proceedings, the general principles on evidence production are to be respected: the

evidence has to be introduced in a public hearing, and the parties must be granted the right for the defence to confront the evidence, granting the opportunity to challenge the authenticity, reliability and integrity of the evidentiary materials.

The production of the evidence will vary depending on whether it is recorded conversations, recorded images or other electronic data.

For telephone conversations, the jurisprudence has required the reproduction of the relevant conversations in the public hearing and/or the reading of the written transcripts, but has also admitted testimony of the person recording the conversations.

For other data, the reading of the transcripts or the reproduction on a computer before the trial court is the usual way to introduce the data as evidence. Alternatively, it is introduced by way of written transcripts. Expert evidence is usually in place too, with the presence of an expert witness to explain the procedure for collecting data and how the integrity, authenticity etc. has been secured.

For the admissibility of intercepted communications as evidence the courts have required (regarding telephone conversations): 1) that the original recordings are made available to the parties, so that they can listen to them; and 2) that the original recordings are complete. These have been considered essential safeguards to guarantee the integrity and authenticity of the evidence, declaring it inadmissible when the conversations were not presented as evidence on the original disks or recording media.

This stance had to be reviewed since the interception of communications by way of SITEL involves, by definition, no "original disk" as the data are directly dumped into a central computer. This means all communications are presented to the court as copies or transcripts.

As to the need to present all the intercepted material, the case law is very clear: the police cannot select conversations or communications but have to transfer all the intercepted material to the investigating judge. All the tapes or disks with the recording of the intercepted conversations or electronic data must be conveyed to the court. For the purposes of using the recordings as evidence at trial, the investigating judge only, and not the police, is allowed to select conversations. Therefore, the police must provide all the recordings with the totality of the conversations, no matter whether they are considered useful for the case or not. Otherwise, the tapes will not be admitted as evidence.

Until now, all the communications recorded were to be disclosed and made available to the defence. This rule has now been limited by the new Article 588*ter* i. LECRIM, that provides that conversations affecting the intimacy of the parties will not be made available to the parties to the proceedings. The parties have to be informed that such parts have been excluded from the copies of the communications they have obtained. It is unclear how this provision will be interpreted and applied.

It is to be welcomed that LECRIM has introduced this rule to better protect the core of the right to intimacy of persons whose communications have been intercepted. However, it will have to be assessed whether those communications affecting the intimacy are relevant as evidence or not and whether a balancing test should be applied. There is no exclusionary rule of evidence based on the protection of the core content of the right to privacy (or intimacy).

2. Inadmissibility of evidence as a consequence of inappropriate collection

The general rules and principles on exclusionary rules of evidence shall apply also to the evidence collected through an unlawful interception of communications. Spanish statutory rules provide for a very strict exclusionary rule. The key statutory provision regarding the exclusion of evidence is Article 11.1 of the Organic Law on the Judicial Power (*Ley Orgánica del Poder Judicial*, LOPJ). The LOPJ was enacted in 1985, one year after the Constitutional Court's landmark decision in STC 114/184, and this decision clearly influenced the wording of Article 11.1 LOPJ, which reads: "Evidence obtained, directly or indirectly, in violation of fundamental rights or liberties, shall have no effect."

The doctrine of the indirect or "reflex effects" (*fruit of the poisonous tree* doctrine) determines the exclusion not only of the main evidentiary elements but also of those other elements of evidence that derive from the original illegal act. The Spanish courts have followed the doctrine of "reflex effects" in those cases where not applying it would result in leaving fundamental rights unprotected. Thus, for instance, recordings obtained through illegal phone tapping are not accepted, neither is the testimony of the officer in charge of the recording, for otherwise the meaning and purpose of the exclusionary rules would be circumvented and it would encourage the adoption of measures that are contrary to the constitutional right to the secrecy of communications.

It has been questioned whether the SC establishes a constitutional right to exclude illegally obtained evidence. Although initially the Constitutional Court considered that such a right was not recognised in the SC, it later decided that a criminal conviction based on evidence gathered in violation of fundamental constitutional rights would undermine the following constitutional safeguards:

The first is the fundamental right to a fair trial recognised under Article 24 SC. The second is the principle of equality of arms, because one of the parties, the prosecution, would be able to use illegally obtained evidence and benefit from the violation of the constitutional rights of the other, the defendant.[44] Finally, the ad-

[44] STC 114/1984, FJ 5. After this judgment, the close relation between the exclusionary rule and the right to a fair trial has been recognised in numerous Constitutional Court decisions. See, e.g., SSTS 768/2007, of 1 October 2007; 48/2013, of 23 January 2013; or 806/2015, of 24 February 2015.

mission of illegally gathered evidence would undermine the presumption of innocence, guaranteed by Article 24. 2 SC. The presumption of innocence in the Spanish legal order, as set out in the ECtHR's case law, not only implies the right to be treated as innocent until a judgment of conviction becomes final, but it also encompasses the right not to be held guilty if there hasn't been sufficient lawfully gathered evidence to prove the defendant's guilt.

3. Use of data outside the main proceedings

a) Data from other criminal investigations

Until Law 13/2015, there was no express rule in LECRIM regarding accidental discoveries, nor on data collected by chance during the interception of communications relating to another criminal offence different from the one for which the judicial warrant was issued. The newly passed provision mainly reflects the principles that had already been adopted by the Supreme Court case law on casual findings. This jurisprudence had evolved mainly within the realm of the execution of home searches, but there was also case law regarding telephone interceptions.

The main principles applicable are summarised next. If the facts discovered are not connected to the offence for which the investigative measure restrictive of fundamental rights was authorised, and those facts appear to be serious enough to justify the adoption of the interception measure, they will serve as "notitia criminis." The authorities carrying out the measure will inform the competent judge about the facts discovered, and a new criminal procedure shall be opened (STS 940/2011, of 27 September), so that the competent judge renders an ex-post judicial authorisation to cover the investigation of the newly discovered offence. However, the original investigating judge can also authorise the extension of the criminal investigation regarding the newly discovered offence.

If the newly discovered facts refer to a crime which would not allow the execution of telecommunications interception, such an offence may only be prosecuted on the basis of the accidental findings if it is connected to the principal offence.[45]

Article 588*bis* i. LECRIM as of 4 October 2015, provides for a special rule on accidental findings regarding another crime during the execution of a measure of telecommunications interception.[46] This rule refers to the requisites set out under Article 579*bis* LECRIM. As a consequence, to proceed with the investigation of the newly discovered crime, an additional judicial warrant needs to be requested.

---

[45] Generally, on the case law of the Spanish Supreme Court on casual findings, see García San Martín, "El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal," pp. 1 ff.

[46] On the admissibility of accidental findings as evidence, see, e.g., SSTC 49/1996, of 25 March 1996; 41/1998, of 24 February 1998.

And it will only be granted if the newly discovered offence justifies the adoption of the measure of interception of communications (penalty higher than three years, or terrorism, or organised crime, or cybercrime or crime committed through internet). It is only by way of this subsequent judicial warrant that the communications can be used for the new procedure and the information obtained can be used as evidence.

Despite the efforts of the legislative to provide for a specific statutory provision to regulate casual findings, in my opinion this rule is still insufficient in practice. Although it is in compliance with Article 4 of the EU Directive 2016/680, taking into account the vast amout of data that can be intercepted, especially through the search of computers (remote or direct), a rule limiting the use of such material as evidence in other criminal investigations or, in other words, in restricting the possibility of using accidental findings of evidence related to other crimes, could be considered. An ex-post judicial warrant for triggering the new investigation might not be enough safeguard against having a kind of review of all the past acts of an individual, as they appear through the stored e-data. In order to avoid such extended powers, users will have to resort to sophisticated encryption tools. But the possibility for the users to establish higher protections regarding their data does not neutralize the depth to which the state can dig into the life of the individuals in searching for any suspect act that may appear when intercepting e-communications.

b) Data from preventive investigations

There are no preventive criminal investigations in the Spanish legal order. As to national security activities and their transfer to criminal proceedings, there are no legal provisions determining how and when this transfer should happen, as has been commented above. As to intelligence activity as evidence, there have been some controversial Supreme Court decisions admitting "intelligence reports" as expert evidence.

The judgment of the Criminal Chamber of the Supreme Court 2084/2001 of 13 December 2001 was the first to qualify intelligence reports issued by the Civil Guard officers on terrorism as "intelligence expert evidence." After this ruling, many more followed the same stance, such as, e.g., STSS 985/2009, of 13 October 2009, 480/2009, of 22 May 2009, or 1097/2011, of 25 October 2011.

However, the doctrine of the Supreme Court on this matter has not been uniform, as there are several rulings stating that the aforementioned "intelligence report" cannot be regarded as expert evidence. See, e.g., SSTS 1029/2005, of 26 September 2005, 556/2006 of 31 May 2006, and 1929/2007, of 16 February 2007.

As far as we know, since 2011 there have been no more decisions dealing with "intelligence expert evidence."

As to other non-judicial preventive investigations, the issue begs the question of the evidentiary value in criminal proceedings of information obtained by way of the execution of supervisory powers and enforcement of compliance programs carried out by compliance officers within companies:[47] as a rule, once a criminal act has been committed no measures restrictive of fundamental rights are allowed by the compliance officer, as he/she cannot act as a kind of private law enforcement agent.[48] And in the case where within its preventive functions any fundamental right is infringed, the general exclusionary rule of evidence of Article 11 LOPJ should apply. Moreover, there is no legal provision that would allow such measures to be carried out within these private investigations, aside from the labour law – for adopting disciplinary sanctions, e.g., – and compliance control.[49]

c) Data obtained from foreign jurisdictions

The traditional rule in international cooperation is that the execution of the requested measures will take place in accordance with the procedural rules of the executing state *(lex loci)*. This has been the rule according to Article 3.1 of the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 20 April 1959.[50] This same rule is found in most bilateral agreements on mutual legal assistance in criminal matters (e.g., Article 5.3 of the Convention with the United States in accordance with EU/US legal assistance agreement that was signed bilaterally with Spain and ratified on 17 December 2004; Article 7 of the Convention on Legal Cooperation and Mutual Assistance between Spain and Brazil of 22 May 2006; Article 10 of the Convention on Mutual Legal Assistance with Mexico of 29 September 2006).

Article 4 of the EU Convention on Mutual Assistance in Criminal Matters of 29 May 2000 introduces the possibility of requesting the compliance with certain formalities of the *lex fori*, which provides that in cases where mutual assistance is granted, the member state shall comply with the formalities and procedures expressly indicated by the requesting member state, unless otherwise provided in the

---

[47] The word "preventive" has to be underlined here. It is considered that within the compliance supervisory functions only preventive actions should be taken. This means that once a criminal act has been committed the criminal investigation is to be handed over to the relevant police and judicial authorities.

[48] STS 2844/2014, of 16 June 2014. No encroachment upon the privacy or the secrecy of the communications is allowed for the compliance officer or the employer: lacking a judicial warrant, such evidence is to be excluded in the criminal proceedings. In the same sense, Colomer Hernández, "Cesión de datos obtenidos a través de sistemas de compliance y procesos penales", pp. 408–421.

[49] In this sense also Colomer Hernández, "Cesión de datos obtenidos a través de sistemas de compliance y procesos penales," p. 424.

[50] On hearing by video and telephone conference see Article 9 and 10 of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, of 8 November 2001.

Convention and provided that such formalities and procedures are not contrary to fundamental principles of law of the member state addressed. Nevertheless, it basically retains the general principle of *lex loci* in the specific regulation of interception of communications contained in Articles 17–22. This is the approach followed also by the EIO Directive (Articles 9.2 and 212.2 Law 23/2014, *in fine*).

The Spanish Supreme Court has repeatedly stated that evidence obtained abroad according to the rules of the executing state is valid in Spain.

Three general principles become evident when analysing the Supreme Court case law in this regard: 1) The evidence obtained pursuant to the procedural rules in the state where it was collected should not be subjected to the test of compliance with the Spanish rules, see, e.g., STS 340/2000, of 3 March 2000 or STS 1142/2005, of 20 September 2005, stating that it is not for the trial court to check whether the evidence obtained abroad complies with Spanish evidentiary rules; 2) it would be possible to check if the collecting of evidence complied with the rules of the executing state, but in such case the burden to prove the infringement of those rules would lie with the party claiming the inadmissibility of the evidence, see, e.g., STS 503/2008, of 17 July 2008; 3) the Spanish Supreme Court has held that for evidence collected in another EU Member State a general principle of trust applies, see, e.g., SSTS 18/2003 of 10 January 2003; 1345/2005 of 14 October 2005; 886/2007, of 2 November 2007: 456/2013, of 9 June 2003; or 116/2017, of 23 February 2017.

There are, however, some comments to be made concerning this general doctrine: First, the Supreme Court after recognising the admissibility of evidence obtained according to the *lex loci* of the executing state, states that this approach is applicable to states that share the same values and principles as Spain as enshrined in the Constitution, so that the requirements for restricting the rights of citizens are substantially similar. Second, for questioning the validity of the evidence obtained abroad it is necessary to provide some objective data suggestive of a possible breach of fundamental rights that is contrary to the constitutional values of the Spanish system (STS 1099/2005, of 30 September 2005).

It is important to note that the vast majority of these decisions analysed evidence obtained implementing the convention on criminal judicial cooperation of the Council of Europe of 1959.

Following the rules set out in the 2000 EU Convention and the aforementioned case law of the Supreme Court in the case of assessing the validity of the telecommunications interception practice abroad, the Spanish trial court has to look at the validity of the national warrant authorising a request of interception to a foreign authority and the content of the letter rogatory, as this has to comply with all requirements that would be necessary if the interception were to be executed in Spain: when the interception of communications is requested through international judicial assistance, Article 18.3 of the 2000 EU Convention requires the

inclusion of the national judicial warrant authorising this measure in the Spanish investigation.

It is different in a case in which evidence is presented as the result of interventions within an ongoing foreign criminal proceeding and not as the result of the international request for cooperation. In these cases, the Spanish courts accept the use of such evidentiary elements obtained in compliance with the *lex loci*. It can be seen that the Spanish Supreme Court has long adopted the principle of mutual recognition, without checking the validity of the evidence obtained abroad, as long as there are no indications of fundamental rights infringements and as long as the foreign country shares equivalent legal values. Nevertheless, in the recent decision 475/2018, of 17 October 2018, the Supreme Court declared that this does not equate to the principle of non-inquiry, which, if applied beyond its formal meaning, would be incompatible with some of the constitutional values (FJ 2).

4. Challenging the probity of intercepted data

As has been pointed out already, Article 588*ter* I LECRIM provides for the full disclosure of communications intercepted, except parts that the investigating judge may exclude to protect the right to intimacy. The full disclosure shall allow the defence to listen to the recorded conversations as well as to analyse the intercepted data.

Defence lawyers in practice usually directly target the form and reasons for the judicial warrant authorising the interception, rather than its technical execution. The lack of enough initial suspicion, the lack of proportionality and in general the lack of sufficient formal motivation for the warrant are frequently invoked arguments against the validity of the interceptions and are also often accepted.

With regard to the technical requirements, defence lawyers do not often invoke such reasons against the admissibility of the evidence: first, because the system SITEL does not cast doubt as to the integrity of the communications intercepted and has been declared in conformity with the constitutional rights by the Supreme Court; and second, because the process of transferring information onto disks is to be done in the presence of the *secretario judicial* (court clerk acting as notary), and the IT expert witness, who can give information concerning the whole process relevant for the authenticity of the data, is also usually involved.

A frequent argument against the admissibility of the evidence obtained by telecommunications interception has also been that the investigators did not present the original disk at court. However, the practice on this requirement differs greatly. Some courts insist on having an original disk and other courts are satisfied with copies of the data.

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

1. International conventions

The European Convention on MLA in Criminal Matters of 20 April 1959 was ratified by Spain on 18 August 1982 (in force since 16 November 1982), and the 2nd Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 8 November 2001, which entered into force in Spain on1 July 2018.

The Convention on MLA in Criminal Matters between the member states of the EU of 29 May 2000 entered into force on 23 August 2005. However, Spain had previously agreed on the provisional implementation of the 2000 Convention, and it was therefore already applicable in Spain even before it had officially entered into force (BOE 15 October 2003).

The UN TOC Convention of 15 November 2000 was ratified by Spain in 2003 (BOE 29 September 2003).

The CoE Cybercrime Convention of 23 November 2001 has been ratified by Spain (BOE 17 September 2013).

2. Bilateral treaties

There are no bilateral treaties providing specific rules on the interception of telecommunications (information provided by the International Cooperation Unit of the General Council of the Judiciary).

3. National regulation

The general rules on international judicial cooperation are provided in Articles 276 to 278 of the Law on the Judicial Power *(Ley Orgánica del Poder Judicial)*. Article 277 LOPJ only states that Spanish courts will provide the international legal assistance requested by foreign judicial authorities in accordance with the Treaties, EU law and other domestic laws. Thus, it is a rule stating the obligation and referring to the applicable laws. Article 278 LOPJ establishes the exceptions to such an obligation, listing the grounds for refusal, which are in short: *ordre public*, exclusive subject-matter jurisdiction of Spain, no jurisdiction of the courts, and non-fulfillment of formal requirements.

Law 23/2014, of 20 November on Mutual Recognition of criminal decisions in the European Union does provide specific rules on judicial cooperation in criminal matters in the EU. This law contains the domestic regulation of all mutual recognition instruments in criminal matters adopted until now. None of the EU mutual

recognition instruments provides for specific rules for the interception of communications, save for the Directive on the European Investigation Order. Until the transposition of the Directive on the EIO into national law by Law 3/2018 of 11 June 2018, the requests for international cooperation for a telecommunications interception within the EU were done via the EU Convention of 29 May 2000 or the MLA Convention of 1959, as far as this rapporteur has been able to confirm (information on bilateral conventions with EU member states that might cover interceptions of telecommunications are unknown to us, but these data have not been definitively confirmed).

B. Requirements and Procedure (Including the Handling of Privileged Information)

1. Incoming requests

The main authorities that are involved in international judicial cooperation in Spain are: 1) the judiciary; 2) the Ministry of Justice; and 3) the Public Prosecution Service. Law enforcement will carry out the measures following the instructions of the judge or the public prosecution. The role of the Ministry of Justice is in general to act as central authority according to the International treaties. The court clerks *(Letrado de la Administración de Justicia)*, who have managerial, procedural and notarial functions within the courts, shall provide support in the handling and execution of requests for international judicial cooperation.[51]

Investigating judges will receive the legal assistance requests directly in all cases where the international conventions or the European instruments so provide. According to the international treaties, however, it is still the general rule that the receiving authority will be the Ministry of Justice, designated as central authority in most international treaties.

In general, once the request has been received – either directly or through the central authority designated in the Conventions or through the National Court or Prosecutor's Office –, Spanish authorities are obliged to execute it. We must recall that the EU Convention of 1959 also allows the direct transmission of the requests in urgent cases (Article 15.2 of the Convention MLA criminal matters of 1959). In these urgent cases, the requests might be sent through Europol.

Under Spanish law, the competence to execute the legal assistance requests in criminal matters lies generally with the investigating judges.

Once the general institutional framework on international judicial cooperation has been described, the specific rules governing the legal assistance within the EU

---

[51] Article 465.8 Judiciary Act and Instruction of the Ministry of Justice 1/2010.

according to the EIO, will be described. The amended Law 23/2014 contains a lengthy provision regarding the competence for receiving and executing the requests for evidence, with telecommunications interceptions included.

While for receiving and executing European arrest warrants (EAW) the Spanish law has opted to centralize the cooperation in the Central Investigating Judge of the National Court (Article 35 Law 23/2014), for incoming EIOs the solution adopted is to designate as exclusive receiving authority the public prosecution. Once received, the public prosecution will register the incoming EIO – which is positive for statistical data – and proceed directly to its execution in those cases where the measure is not restrictive of fundamental rights (Article 187.2 Law 23/2014).

If the measure to be executed is restrictive of fundamental rights (according to Spanish law, these measures are the ones that are subject to prior judicial authorisation), the public prosecutor cannot execute it by him- or herself. In such a case – and this is the case for the interception of telecommunications as a rule –, the EIO shall be transmitted to the competent investigating judge. It shall be forwarded to the judge also in cases where the requesting authority specifically so demands, even if the measure to be carried out does not imply limtations of fundamental rights according to Spanish law. According to the rules on subject-matter and territorial competence, the public prosecutor will send the request to: 1) either ordinary courts or the National Court or to juvenile courts; 2) of the territory where the investigative measure is to be carried out; or subsidiarily, where there is any territorial connection with the crime, the suspect or the victim. In cases where no connection with a certain territory is identified, then the territorial competence will lie with the Central Investigating Judge within the National Court. If the EIO includes several investigative measures to be executed in different territories, the public prosecutor will send the EIO to the one competent according to the said territorial criteria.

Finally, the General Council of the Judiciary *(Consejo General del Poder Judicial)* gives support in mutual legal assistance proceedings through its unit on international relations. This unit not only provides support to the national courts when acting as issuing or executing authority, but it also coordinates the national network of judges specialised in international judicial cooperation.[52] Any Spanish judge that requires it will be assisted by the General Council in the correct transmission and effective execution of international legal assistance requests.[53] Furthermore, the Council has published an online guide which contains the complete regulation –

[52] The organisation of this unit has been regulated in more detail recently by way of an internal Regulation of the General Council of the Judiciary "On International Judicial Cooperation and Judicial Networks," Reglamento 1/2018, approved by the GCJ on 27 September 2018.

[53] Articles 71 and ff. of the Reglamento 5/1995, of 7 June, de los aspectos accesorios de las actuaciones judiciales.

listing all the bilateral and multilateral conventions, as well as the EU instruments and their transposition to Spanish domestic law –, practical explanations on how to manage legal assistance requests, and standard forms and information on how to communicate with the contact points of the European and the Spanish Judicial Networks.

2. Outgoing requests

The investigating judge carrying out the investigation of the offence is competent to issue the international cooperation request (Article 187.1 Law 23/2014, 20 November in connection with Article 303 LECRIM, which regulates the competence of the investigating judge to carry out the pre-trial criminal investigation). If the measure has been requested once the trial has started, the competent authority will be the trial court.

Within the realm of its competences, the Spanish public prosecution also has the competence to issue outgoing requests within the judicial cooperation regulated under Law 23/2014, as it is defined as "judicial authority" in the context of the EU instruments of mutual recognition in criminal matters. For issuing an EIO Article 187.1.II expressly provides for this power of the public prosecutors in cases where the measure is not restrictive of fundamental rights. As a rule, public prosecutors can issue an EIO to carry out investigative measures they could order within Spain under Spanish law.

3. Technical regulation

There are no legal provisions on the filtering of incoming data or of outgoing data, or on the way the transfer of the information is to be carried out. Within the EU, the secured intranet of the EJN could be used. While the Law 3/2018 transposing the EIO Directive and amending the Law 23/2014 has included a new provision titled "Transfer of the evidence obtained" (Article 211), this provision does not foresee the way in which the evidence is to be transferred, but only the timing –as a rule immediately–, the circumstances in which the transfer can be suspended and how to proceed in cases where the evidence is also needed within a national criminal proceeding.

In practice, the transfer takes place in different ways: it was not unfrequent that a member of the judicial police or even a member of the public prosecution would travel abroad to fetch the disks with the recorded communications and bring them to the Spanish investigating judge. This is still often done when the Spanish officers have already travelled to the relevant country for purposes of the investigation, but in the past there were also cases where the travel took place only for bringing the elements of evidence. This is, however, becoming less frequent in practice. With countries where there is a liason magistrate (e.g., with France, where there is

one in Madrid as well as in Paris), the transfer of the data is often done through them. The National Court reports cases where the data have been transferred through an Embassy (they refer to single cases of data transfer with the USA). In investigations where several EU countries are involved and joint investigation teams have been set up, the disks sometimes are transferred through the heads of the respective joint investigation teams. In other cases, the disk is attached to the documents related to the request and sent by ordinary channels.

In sum, there is still no completely uniform practice, although the transfer by electronic means is increasing.

4. Real-time transfer of communication data

As far as we know, at present neither the current legal framework nor the technical setting allows for the judge from another EU Member State to have direct access to the data resulting from the telecommunications interception.

C. European Investigation Order

The EIO was transposed into the Spanish legal system by Law 3/2018 of 11 June, amending the Law 23/2014, of 20 November 2014 on Mutual Recognition of criminal decisions in the European Union. This law sets out the general principles applicable to the mutual recognition principle in criminal matters in the EU and it includes in one single legal instrument the diverse legal provisions transposing the EU instruments on judicial cooperation in criminal matters. It provides for the domestic regulation of the EU evidence warrant, and regulates the EIO under Articles 186 to 223.

The rules on the EIO closely follow the text of Directive 2014/41/EU, although the grounds for refusal have been transposed as mandatory, and not as possible grounds for refusal, as provided under Article 11 EIO Directive (see Article 221.1 Law 23/2014 with regard to the interception of telecommunications). The transposition of this Directive has not caused any further legal amendements with regard to the interception of communications.

Law 23/2014 regulates the execution of an EIO requesting the interception of communications, establishing:

> **Article 221. Execution of a European investigation order on interception of telecommunications**
>
> 1. The Spanish competent judicial authority shall refuse to execute the European investigation order, in addition to the reasons provided for in article 32, paragraph 1, and article 207, in cases where the investigative measure would not be authorized in a similar domestic case.
>
> 2. When the Spanish competent judicial authority receives a European investigation order for telecommunications interception, it may execute it in one of the following ways:

a) Immediate transmission of the telecommunications to the issuing authority.

b) Intervention, registration and subsequent transmission of the result of the telecommunications intervention to the issuing authority.

The choice of how the European investigation order will be executed will be agreed with the issuing authority.

Spanish authorities will recognize and execute the EIO unless they find that there is a ground for refusal. Grounds for refusal are listed under Article 207 Law 23/2014 with a similar wording as in Article 11 EIO Directive, but, as already mentioned, as mandatory grounds for refusal. A main issue that has been already raised is the interpretation of Article 10.5 EIO Directive (Spanish Article 206 Law 23/2014), which provides that when the investigative measure indicated in the EIO "would not be available in a similar domestic case" and there is no other measure that can substitute it, the executing authority shall notify the issuing authority that "it has not been possible to provide the assistance requested."

The expression of "similar domestic case" has raised the question of whether the executing authority shall check the sufficiency of the grounds that led to the issuing of the EIO. According to Spanish constitutional case law, mere suspicions or intelligence information are not enough for permitting the encroachment of the right to the secrecy of the communications; instead, strong indications are required for this very intrusive measure to be authorised.

The question is: if intelligence information would not be enough for granting the interception of communications in a "similar domestic case," should the enforcement of an EIO based on such information then also be refused? This interpretation would run counter the principle of mutual recognition, which would not allow for checking the reasons that led the requesting authority to consider the requested measure proportional and necessary. Nevertheless, among the Spanish practitioners the opinions are not uniform, and it is discussed to what extent the principle of mutual recognition could lead to setting a lower standard for interception of communications carried out in execution of an EIO than would be applicable for a purely domestic interception.

Regarding the interception of communications which do not require the technical assistance of the state where the communications are being intercepted, the amended Spanish Law 23/2014 – which follows Article 31 EIO Directive – states:

Article 222. Notification to Spain of the interception where the subject of the interception is in Spain, and where its technical assistance is not necessary

Upon receiving the notification that an interception of telecommunications of a suspect or prosecuted person is taking place in Spanish territory, and the said intervention would not be authorised in a similar domestic case, the competent Spanish authority shall notify the state that is executing the interception, without delay and no later than 96 hours after receipt of the notification:

a) That the interception cannot be carried out or shall be terminated;

b) And, where appropriate, that the material already intercepted while the person subject to the interception was in Spain may not be used, or may only be used under con-

ditions which it shall specify. The competent authority of the intercepting state shall be informed of the reasons justifying such conditions.

The practice regarding this obligation to notify the "intercepted" state, as was already established under the EU Convention of 2000, has led to a diverse practice: judges of the National Court state that some states have regularly complied with these notifications, whilst notifications from other states have never been received (not being able to establish whether the lack of notifications was due to the absence of interceptions or for other reasons). As a rule, Spanish notified authorities (National Court) adopted a flexible approach towards these interceptions, not being aware of any case where the Spanish authority had ordered the intercepting state to stop the interception.

According to the EIO Directive and the Spanish Law 3/2018 transposing it, if, in accordance with the domestic law of the state where the telecommunications were intercepted, the authorities decided that such measure would not be authorised in a similar domestic case, then the investigative measure would not comply with the *lex loci*. As explained already, in such a situation the "notified state" *may* prohibit the measure or the use of the data obtained thereby.

There is no case law yet regarding what the consequences in Spain would be if the "notified state" were to prohibit the use of the intercepted communications. Would Spain as "intercepting state" be bound by such a decision? Would such a decision render the evidence obtained in the foreign state inadmissible in the *forum* state? These are questions that will need to be faced by the courts in practice. In our opinion, in those cases where technical assistance is not needed for the interception of communications, the member states should adopt a flexible stance and try not to make use of the possibilities of prohibiting those measures or the evidence obtained "if they would not be authorised in a similar domestic way." In this sense, we are in favour of not trying to impose territorial boundaries and too strict concepts of sovereignty in cyberspace.[54]

D. Statistics

As for the EIO, during 2017 (from May to December) 186 EIOs were received in Spain, and in 2018, until 1 October 2018, there were 944. The statistics up to now do not specify what kind of evidence or investigative measure was requested, so one cannot identify how many requests for interception of communications were received or issued.

---

[54] See Bachmaier Winter, "Mutual recognition and cross-border interception of communications: the way ahead for the European Investigation Order," pp. 332–334.

Bibliography

Aguilera Morales, *Las diligencias de investigación fiscal*. Madrid 2014.

Bachmaier Winter, "Información de inteligencia y proceso penal" in *Terrorismo, proceso penal y derechos fundamentales*, ed. L. Bachmaier. Madrid-Barcelona 2012, pp. 45–101.

Bachmaier Winter, "Intervenciones telefónicas y derechos de terceros en el proceso penal. La necesidad de una regulación legal del secreto profesional y de otras relaciones de confianza," *Revista de Derecho Procesal* (2004/1-3), pp. 41–82.

Bachmaier Winter, "Mutual recognition and cross-border interception of communications: the way ahead for the European Investigation Order", in *The needed balances in EU Criminal Law*, in Weyembergh et al. (eds.). Oxford 2017, pp. 313–336.

Bachmaier Winter, "Remote search of computers under the new Spanish Law of 2015: proportionality principle and the protection of privacy." *ZStW*, 2017, 129(1), pp.1–27.

Barnes Vázquez, "Introducción al principio de proporcionalidad en el derecho comparado y comunitario, *Rev. Actualidad Penal* 135 (1994), pp. 495–522.

Bernal Pulido, *El principio de proporcionalidad y los derechos fundamentales*. Madrid 2003.

Colomer Hernández, Cesión de datos obtenidos a través de sistemas de compliance y procesos penales, in Colomer Hernández (dir.), *Cesión de Datos Personales y Evidencias entre Procesos Penales y Procedimientos Administrativos Sancionadores o Tributarios*. Cizur Menor 2017, pp. 367–431.

Gimeno Sendra, "Las intervenciones telefónicas en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo", *La Ley* 1996-2, pp. 1617–1624.

González Beilfuss, *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional*. Cizur Menor 2003.

González Cano, "Cesión y tratamiento de datos personales, principio de disponibilidad y cooperación judicial en la Unión Europea", in Colomer Hernández (dir.) *Cesión de Datos Personales y Evidencias entre Procesos Penales y Procedimientos Administrativos Sancionadores o Tributarios*. Cizur Menor 2017, pp. 41–80.

Heredero Higueras, *La Directiva Comunitaria de proteccion de datos de carácter personal*. Madrid 1998.

Manso Porto, "Las escuchas telefónicas entre abogado defensor y cliente en una comparación internacional," *Estudios Penales y Criminológicos USC*, vol. XXXII (2012), pp. 39–95.

Marchena Gómez/González-Cuéllar Serrano, *La reforma de la Ley de Enjuiciamiento Criminal de 2015*. Madrid 2015.

Martín Casallo, "Implicaciones de la Directiva sobre protección de datos en la normativa española" in *X años de Encuentro sobre Informática y Derecho*. Pamplona 1997.

Montón Redondo, "Las interceptaciones telefónicas constitucionalmente correctas", *La Ley,* 1995-4, pp. 1043–1052.

Ortí Vallejo, *Derecho a la intimidad e informática*. Granada 1994.

Oubiña Barbolla, "Datos personales y nuevas tecnologías de investigación tecnológica: oportunidades, retos y límites", en Colomer Hernández (dir.) *Cesión de Datos Personales y Evidencias entre Procesos Penales y Procedimientos Administrativos Sancionadores o Tributarios*. Cizur Menor 2017, pp. 221–277.

Pedraz Penalva/Ortega Benito, "El principio de proporcionalidad y su configuración en la jurisprudencia del Tribunal Constitucional y en literatura especializada alemana," *Rev. Poder Judicial* 17 (1990), pp. 69–100.

Rodríguez Laínz, "Consideraciones jurídicas en torno a la licitud constitucional de SITEL," *La Ley* Nº 7344, Sección Doctrina, 17 Feb. 2010, pp. 1–29.

García San Martín, "El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal", *La Ley* 4917/2014, pp. 1–7.

Serrano Pérez, *El derecho fundamental a la protecciónnd e datos. Derecho español y derecho comparado*. Madrid 2003.

Troncoso Reigada, "Protection of data in e-government" in the foreword to the study coordinated by the Data Protection Agency of Madrid and published under the title e-Prodat: e-Government and Data Protection in European Regions and Cities. Madrid 2006.

Vidal Fueyo, "El principio de proporcionalidad como parámetro de constitucionalidad de la actividad del juez", Anuario de Derecho Constitucional Latinoamericano 2005.

Zoco Zabala, *Nuevas tecnologías y control de las comunicaciones*. Madrid 2015.

List of Abbreviations

BOE	Boletín Oficial del Estado
CC	Criminal Code
CNI	Centro Nacional de Inteligencia (National Intelligence Centre)
DEA	US Drugs Enforcement Agency
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EIO	European Investigation Order
EJN	European Judicial Network
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
LECRIM	Ley de Enjuiciamiento Criminal (Spanish Criminal Procedure Code)
LOPJ	Ley Orgánica del Poder Judicial (Organic Law of the Judicial Power)
MLA	Mutual Legal Assistance
R.D.	Royal Decree
RJ	Referencia Jurisprudencia

SC	Spanish Constitution
SITEL	Sistema integrado de interceptación legal de las telecomunicaciones (comprehensive system for intercepting electronic communications)
STC/SSTC	Sentencia/s Tribunal Constitucional
STS/SSTS	Sentencia/s Tribunal Supremo

Sweden*

National Rapporteur:
Iain Cameron

* This report outlines the legislation and case law as of April 2019.

Contents

Introductory Note

References to the Swedish statute book (SFS) are by year of enactment followed by the relevant number. I use the short form of citation of a provision in a statute which is otherwise rather cumbersome in English, thus, Chapter 2 section 1 paragraph 1 point 1 is cited as 2:1, para 1, p. 1. Where a section has only one paragraph but several points, the paragraph number is omitted.

As regards interpretation of legal provisions, there is relatively little case law in this area. Cases from the Supreme Court are cited from the semi-official series *Nytt Juridisk Arkiv* (NJA). Unreported cases from courts of appeal – which have a low value as precedents – are cited by case number and date. There are some decisions from the Ombudsman, and more recently, from the oversight body, SIN (see below). In Swedish legal culture, the courts place considerable significance on the historical interpretative method, and so the *travaux préparatoires* are regarded as an authorative source. Having said this, in criminal law the textual method of interpretation (objective wording of the provision) is at least as important. References to *travaux préparatoires* are either to the number of the commission responsible for investigating the law, *Statens offentliga utredningar* (SOU) or *Departements serien* (Ds) and the year of its report, or the number of the bill (proposition) put before parliament in the parliamentary year in question. The majority of provisions are regulated in considerable detail in the Code of Judicial Procedure (*Rättegångsbalken*, CJP). A translation of this was produced in 1998, but so many provisions have changed, that all the translations used in the present report are my own.

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Security Services with Powers of Telecommunication Interception

1. National security architecture

Sweden has a national police force, administratively divided into seven regions and subdivided into smaller areas. There is a separate customs service, with responsibility for, *inter alia*, investigation of smuggling offences. Since 1 January 2015 the police and Security Police have been separate entities. The Security Police is now a largely civilian security agency, but it also has certain police powers. Sweden has a signals intelligence agency, *Försvarets radio anstalt* (FRA). All four of these administrative agencies can engage in interception of telecommunications.

Thus, in Sweden communication interception is possible under three different legal regimes: (repressive) criminal law, (preventive/investigative) police law, and intelligence (or state security) law.

2. Powers for the interception of telecommunications

a) Law of criminal procedure

Interception of telecommunications by the police, and Security Police in the context of criminal investigations, is regulated in the Code of Judicial Procedure or *Rättegångsbalken* (CJP) (1942:740). Relaxations of the normal rules in the CJP for the Security Police in certain circumstances are set out in the Act (2008:854) on measures to investigate certain societally dangerous crimes.

b) Preventive law

Proactive interception by the police or Security Police (which is rare) is provided for in the Act (2007:979) on measures to prevent particularly serious crimes. In addition, the police and Security Police, prior to opening a preliminary investigation, have access to metadata for intelligence purposes as regards investigating more serious offences. This is regulated under the Act (2012:278) on the collection of data on electronic communications in law enforcement intelligence.

c) Law of intelligence agencies

The signals intelligence agency, *Försvarets radio anstalt* (FRA), is permitted to intercept international communications (metadata and content data). This is permitted subject to certain conditions, but only for intelligence purposes under the Act (2008:717) on communications interception for defence intelligence purposes.

d) Customs Investigation Service

The customs service has access to interception of telecommunications under the same conditions as the police, i.e., interception for the investigation of criminal offences, regulated in CJP and of metadata for intelligence purposes, regulated in the Act (2012:278) on the collection of data on electronic communications in law enforcement intelligence.

The results of specific interception measures under these different regimes can be exchanged between the Security Police, the customs, and the police. Moreover, the results can be exchanged with competent authorities in other countries. Both types of exchange are governed by the Transparency and Secrecy Act (2009:400). This provides, *inter alia*, that an administrative agency can transfer secret information to another administrative agency if this is necessary in order for the trans-

ferring agency to fulfil its functions as set out in statute or subordinate legislation (Chapter 10 section 2). Thus, transfer is possible between customs, the police, and the Security Police, and between these agencies (and the signals intelligence agency). This basis for exchange of information is in addition to exchanges carried out as a result of interceptions made on behalf of a police force in a foreign (usually EU) state under mutual assistance legislation.

3. Responsibility for the technical performance of interception measures

Telecommunications data is physically held by different telecommunications companies. The court where the criminal investigation is taking place issues a warrant requiring the telecommunications company to give the police or Security Police access to specified teleaddresses or specified historical or real-time telecommunications records. The prosecutorial authority is organised in the same way as the police, i.e., with a central unit in Stockholm and seven regional offices. The Security Police is also a national organisation, with regional offices. The Security Police has the technical expertise in this area, so it handles the technical aspects of interception even for the police, transferring the requested data to them. When the Security Police collects its own data, it applies for court warrants through a specialised prosecutorial chamber based in Stockholm.

For signals intelligence, the law requires telecommunications companies to route all international communications through certain connecting points which have been placed under the physical control of an independent oversight body, *Statens Inspektion för Underrättelsearbete* (SIUN). If the Defence Intelligence Court has issued a warrant for interception of particular cables for particular purposes, SIUN permits FRA access to the signal bearers in question, for the specified purposes.

B. Statistics on Electronic Communication Interception

1. Obligation to collect statistics

There is an obligation on the police and Security Police to report statistics every year to Prosecutorial Authority, which produces a public report the year after (for 2015 on 30 May 2016, Report ÅM-A 2016/0093, for 2017 Report ÅM-A 2017/2170). The statistics as regards the Security Police are aggregated for secrecy reasons. Disaggregated statistics are reported to the oversight body (the Commission on Security and Integrity Protection, SIN). The signals intelligence agency reports statistics to the oversight body (SIUN) but these are not made public.

2. Current data

As far as the police and customs are concerned, during 2016, 1235 people had the content of their telecommunications intercepted, and 2022 people had their metadata intercepted. During 2017, 1378 people had the content of their telecommunications intercepted, and 2162 people had their metadata intercepted There is overlap between these two figures, i.e., the same person could have been subjected to both (metadata interception is included in a warrant to intercept content, but not vice versa).

II. Principles of Telecommunication Interception in Constitutional and Criminal Procedural Law

A. Constitutional Safeguards of Telecommunication and the Constitutional Proportionality Principle Regarding Access to Data

Under the Swedish Constitution (Instrument of Government (IG) 2:6 para 1), there is protection "against body searches, house searches, and other such invasions of privacy, against examination of mail or other confidential correspondence, and against eavesdropping and the recording of telephone conversations or other confidential communications." Under 2:6 para 2 "everyone shall be protected in their relations with the public institutions against significant invasions of their personal privacy, if these occur without their consent and involve the surveillance or systematic monitoring of the individual's personal circumstances." The right under IG 2:6 para 2 is relative, meaning it can be limited by statute. There is no irreducible core and absolute right of privacy. The right under IG 2:6 para 2 is also comparatively new, dating from 2011. Historically, freedom of information and freedom of expression have been more strongly guaranteed than privacy and data protection. There is no express constitutional right to informational self-determination, though it can be seen as an implicit part of the right to personal integrity.

Under IG 2:20 limitations in IG 2:6 and other relative rights (listed in IG 2:20) "may be imposed only to satisfy a purpose acceptable in a democratic society. The limitation must never go beyond what is necessary with regard to the purpose which occasioned it, nor may it be carried so far as to constitute a threat to the free shaping of opinion as one of the fundaments of democracy. No limitation may be imposed solely on grounds of a political, religious, cultural or other such opinion." This constitutional principle is mainly aimed at the legislature, in drafting legislation, however, it has on occasion been applied by the courts. CJP 27:1 (below) is invoked much more frequently.

B. Statutory Protection of Personal Data, Oversight and Consequences for the Unlawful Infringement of Telecommunications

Personal data is generally protected by the principle of "purpose limitation of personal data," which is expressed in the GDPR. As regards telecommunications companies and staff, the Electronic Communications Act (2003:389) (hereinafter, ECA) provides for duties of confidentiality and also for exceptions to this duty, as regards revealing data to law enforcement personnel (when this has been duly authorised). Where the police have obtained telecommunications data, or stored personal data, the police are themselves under obligations in the Police Data Act not to disclose this except where this is necessary for criminal investigation.

Seizure of a computer in order to access data stored upon it is governed by similar rules as the seizure of a physical document, meaning that CJP 27:2 applies. This provides that "If it can be assumed that a document contains information that an official or other person may not disclose under testimony under Chapter 36 section 5, the document may not be seized from the possession of that person or the person who is owed the duty of confidentiality. Nor may from the person of the suspect or his relative, as defined in Chapter 36 section 3, written communications between the suspect and his relative or between such relative be seized, except if the issue concerns an offence in respect of which a less severe penalty than imprisonment for two years is not prescribed."

As regards the consequences of these safeguards for the interception of (electronic) communication, the primary protection is preventive, in logging routines, etc. The Data Protection Inspectorate has oversight of all data registers, including those of the police and Security Police. The police have been criticised on occasion for deficiencies in data registers (overlong retention of information, registering of information on ethnic origin etc which should not have been registered). In addition, a special body, the Commission on Security and Integrity Protection (*Säkerhets och integritetsskyddsnämnden*, SIN) has oversight of both the police and Security Police registers and can receive complaints from the public. SIN also has a follow-up oversight of coercive measures and access to metadata. Criminal penalties for breach of confidentiality requirements by the police or telecommunications staff are to be found in the ECA and the Transparency and Secrecy Act (2009:400), which in turn makes reference to Criminal Code (CC) (1962:700). The offences in question are misuse of office (CC 20:1) and breach of official secrecy (CC 20:3). A few police every year are prosecuted for misuse of office, due to unauthorised access to information.

C. Powers in the Code of Criminal Procedure

Coercive powers in the Swedish criminal procedural law are based on differentiated, precise, and specific provisions. An analogous application of coercive powers is not possible. The principle of "legal security" *(rättssäkerhet)* is fundamental to Swedish criminal law and criminal procedure. It is only partially codified; the constitutional rights in IG 2:8-10 since the reform of 2010 have been grouped together in the Instrument of Government under the subheading *rättssäkerhet*, but there is no definitively agreed content to the concept and sections 8–10 IG certainly do not exhaust it. It includes the need for criminalisation and coercive state measures to have clear support in law.

Having said this, the fact that interception and surveillance are both defined in technique neutral ways (see below) means that new techniques for obtaining data can be used within existing legal provisions. These new techniques, perhaps together with changed social habits (e.g., not turning off one's mobile phone, meaning that a "temporary" dynamic IP address "lasts longer") can mean that considerably more personal data becomes available, without the need for a change in the law. The CJP provides for a sliding scale of authorisation as regards what are called "coercive measures" *(tvångsmedel)*.[1] There is no definition of "coercive measures" in the CJP but it is often defined in doctrine and the *travaux préparatoires* as being a direct intervention against a person or property within the exercise of public authority and with the character of an intrusion in the personal integrity of the individual.[2]

Under CJP 27:1 there is a general rule of proportionality applying to all coercive measures: "The coercive measures described in this chapter may be imposed only if the reasons for the measure outweigh the consequent intrusion or other detriment to the suspect or to another adverse interest." As regards specific categories of protected communications, under CJP 27:22 "Telephone conversations or other telecommunications between the suspect and his defence counsel may not subject to secret wiretapping. If during the tapping it appears that it is such a conversation or communication, the surveillance shall be discontinued. Recordings or notes, to the extent that they are subject to the prohibition, shall immediately be destroyed." Other privileged categories of communications are those between a priest or doctor and a suspect.

---

[1] The interception of metadata has so far not been regarded as a sufficiently serious interference with personal integrity as to be seen as a "coercive measure," although analogous levels of safeguards apply (see further below).

[2] See, for example, SOU 1995:47 p. 137, Bill 2005/06:178 p. 21 and, generally, Lindberg, G., *Straffprocessuella Tvångsmedel* (Coercive measures under the law of criminal procedure), 3 uppl. Karnov, 2013. Coercive measures can be open, such as search, seizure or body search, or covert, such as interception of telecommunications.

Which coercive measures can be used is dependent upon the seriousness of the material offences under investigation: where stiffer sanctions apply, more coercive measures are available.

A preliminary inquiry into a criminal offence is to be initiated, and led, by the police or a prosecutor if information is received that a crime has been committed (CJP 23:1). If an investigation has been initiated by the police and the matter is not of a simple nature, the prosecutor is to assume responsibility for conducting the investigation as soon as someone is reasonably suspected of the offence. The prosecutor is also to take over the conduct of the investigation if special reasons so require (CJP 23:3). In practice, the question of who shall lead the investigation in a particular case is often solved informally, although the prosecutor always has the last word. The percentage of investigations led by the prosecutor varies considerably according to the type of offence in question, with the majority of investigations into serious offences being led by the prosecutor.

III. Powers for Accessing Electronic Communications Data in the Law of Criminal Procedure

A. Overview of the Legal Framework and the Respective Provisions in Criminal Procedural Law

Most of the relevant provisions are set out in considerable detail in Chapter 27 CJP. No additional general clauses are applicable.

B. Interception of Content Data

1. Scope, object and temporal limits

The main provision in criminal procedural law dealing with the interception of the content of communication in transmission is CJP 27:20 which provides that:

> Covert interception of electronic communications and covert surveillance of electronic communications shall, unless otherwise provided in the second paragraph, only occur if someone is reasonably suspected of the offence and the measure is of particular importance to the investigation. This measure may only relate to
>
> 1. a phone number or address, or a certain electronic communication during the time of the authorisation which is held or has been held by the suspect or which may otherwise be assumed to have been used or may be used by the suspect, or
>
> 2. a phone number or address, or a certain electronic communication if there is particular reason to assume that the suspect during the time of the authorisation has or will contact this number etc.
>
> Secret surveillance of electronic communication shall, in addition to what is stated in the first paragraph, be carried out in order to investigate who may reasonably be suspected

of the crime, if this is of particular importance to the investigation. However, only data relating to the past may be collected.

As regards the object of interception, the definitional provisions are in two different Acts. CJP 27:18 provides that "Covert interception of an electronic communication means that the content of a message which in an electronic communications network is being or has been conveyed to or from a telephone number or other address, is covertly listened to or intercepted by technical means." The ECA 6:1 defines electronic communication and provides: "electronic communication means any information exchanged or transmitted between a limited number of parties through a publicly available electronic communications service, except information which is transmitted as part of the broadcasting of radio and television programs that are targeted to the general public […]." This should be read together with the definition in 1:7 of the same Act, namely "electronic communications network means transmission systems and applicable equipment, switching or routing equipment and passive network elements and other resources which permit the transfer of signals, by wire or radio, by optical or by other electromagnetic means, independently of the type of information transmitted."

As regards temporal limits, warrants are for a maximum period of one month (CJP 27:21, para 2). This period can be renewed.

A warrant is not needed for the interception of communications which are purely by radio, but as mobile phones communicate partly by radio and partly by cable, the full body of legal safeguards applies to these.

All of the following contents of traffic can be captured under Swedish criminal procedural law:

– analogue communication (voice and data) via landlines;
– IP traffic of a person-to-person communication;
– IP traffic between a person and an automated information system (such as communication with a webserver while downloading from a website);
– IP traffic between a person's computer and their data storage in a cloud or other remote storage of data processing systems;
– IP traffic between two independent computer systems (e.g., between an automated machine and its computer-based automated control centre, especially in the "internet of things").

As regards the third of these, communication between a personal computer and the cloud, it should be added that the content of information which is stored on the cloud can only be accessed via a warrant for interception of electronic communication.[3]

---

[3] Bill 2002/03:74, p. 88, and Lindberg, op. cit., p. 500.

Both stored data and data in communication are protected, meaning that a warrant is necessary to access both. If the email which the police wish to search has been received by and is stored on the suspect's computer, or if a text message (SMS, MMS) is retained on the suspect's mobile phone, an alternative method is to seize the computer or mobile phone and access the email or SMS/MMS message.

2. Special protection of confidential communication content

The CJP provides for specific safeguards excluding particular types of information from electronic communication interception. Under CJP 27:22 covert interception of electronic communications must not refer to phone calls or other messages where someone expresses himself/herself if the person in question could not be heard as a witness (CJP 36:5) If the interception is ongoing it must be immediately interrupted. If recordings have been made, these must be immediately destroyed.

Where a person argues that privileged data is kept on a computer or a mobile phone (e.g., the suspect is a journalist), then the search must occur in the presence of the suspect's lawyer.[4]

The law regulating financial and banking secrecy does not contain special protection for communications.

There is no special protection for communication in a "core area of private life" (e.g., prayers, communication during sexual activities, diaries, etc.) except where it falls under CJP 27:22/36:5 (above). The latter provision provides *inter alia* that "Anyone who is a priest or performs a similar function in a religious community may not be heard as a witness concerning something he or she has learned during confession or individual counselling." As regards communication during sexual activities, diaries, etc., these communications would normally not be necessary for the investigation of the offence, and so would routinely be destroyed after the preliminary investigation is concluded (CJP 27:24).

There are a small number exceptions which are set out in CJP 36:5 detailing when people who have privileged communications nonetheless may be called upon to testify.

There are no legal differences between handling analogue and digital communication, but an important technical one in that real-time monitoring (and so switching off of interception) of some forms of digital communication is not possible.

The person leading the investigation determines whether a person is entitled or not to privileges. Such a decision is made under criminal responsibility (i.e., it will

---

[4] Ombudsman decision 1724-2011, 2012-04-25, see also Court of Appeal for Northern Norrland, Mål nr Ö 198-15, judgment 2015-03-26.

be misuse of office to take an unjustified decision in this respect, although having said this, the threshold for "misuse" is set relatively high). As noted already (in answer to question 4b), it will usually depend on the seriousness of the case whether the person leading the investigation is a prosecutor or a senior police officer. In either case, this person determines which other people involved in the investigation are permitted to access the data collected (CJP 27:12). The court in the subsequent trial also has access to all data not immediately destroyed as irrelevant or as privileged. The internet provider simply receives the order to hand over specified data, without any explanation, and has no discretion to determine whether it may be handed over or not.

3. Execution of telecommunications interception

The standard mode of interception is for the police, customs or Security Police to order telecommunications providers to extract and surrender specific communication. The police, customs, and Security Police do not intercept specific communication themselves and without recourse to third parties (although see below, regarding proposals for hacking).

For signals intelligence collection (i.e., not applicable for the investigation of specific crimes) SIUN gives the signals intelligence agency access to the signal bearers (the fibre optic cables). Once this has been done, FRA can access the data without the participation of the telecommunications companies.

As has already been mentioned, the Security Police handle the technical aspects of interception on behalf of the police and customs. The Security Police do not have direct access to telecommunications companies' cables, etc. Once a court order has been issued to the telecommunication companies, the Security Police instruct the company either to hand over requested data or to connect the listed numbers (IP addresses, etc.) to the Security Police equipment.

As regards which types of accompanying investigative measures are permitted in Sweden, with court permission, clandestine access to plant a bug is permissible (although the expense and other technical difficulties involved means that this happens only rarely in practice). A by-product of this can be the interception of electronic communications. The police, Security Police, and customs do not yet have the power to use remote forensic software (hacking techniques) or key loggers as such. However, the increased use of encryption has led a Commission of Inquiry[5] to recommend introducing this power and a legislative proposal on the matter is expected in 2019. If, as seems likely, the proposal is passed, a court will give approval (on application by the prosecutor) for hacking to be used to investigate a small category of offences. Similar conditions as for bugging are likely to apply.

---

[5] See SOU 2017:89.

Hacking using both hardware (key loggers) and software (Trojans), is likely to be permissible. The Commission of Inquiry estimated that hacking would not be used particularly often: around 30 times per year.

The definition of "public communications network" in ECA 1:7 is: "an electronic communications network which is wholly or mainly used for the provision of publicly available electronic communications services and which supports the transfer of information between network connection points." ECA 2:1 specifies that any person or company which provides public communications network services is obliged to seek a licence from the Post and Telecom Authority (*Post och telestyrelsen*, PTS). This definition will presumably cover companies which provide services at a "deeper" level (IP transport level, etc.) even if it is assumed that it will be only rarely that such a provider will be ordered to implement electronic communications interception or electronic communications surveillance.

As regards rules in the situation when the intercepted device is located in another country or if the location of the device is unknown (e.g., satellite communications), the situation is today only partially regulated. For non-EU states (as well as for Denmark and Ireland) the Act on Mutual Legal Assistance (Chapter 4 section 26) provides that a prosecutor can request the (legal or technical) assistance of a foreign state to intercept the communications of a person who is in another state. The other state may require that a Swedish court must first have approved this, and in such cases, the court is to decide whether to grant the prosecutor's request on the same conditions as would apply for a warrant issued for interception of communications in Sweden. For EU states under the Act (2017:1000) on a European Investigation Order, where a Swedish prosecutor has applied for and received a EIO for the purpose of interception of communications, but the state implementing the order (State A) is able to, and does, intercept some or all of these communications in another EU state, B, then State B is to be informed of the ongoing interception. If State B, within 96 hours, requires this to cease, then the prosecutor is to annul the Swedish decision authorising the interception (Chapter 4 section 12).

The legislative proposal which is expected in 2019 regarding hacking is likely to introduce a possibility unilaterally to issue a warrant for hacking of devices situated abroad, or where the location is unclear ("loss of location").

4. Duties of telecommunication service providers to cooperate

The cooperation duties of internet providers are set out in ECA 6:16a which provides that:

> Anyone who conducts activities that are subject to notification under 2:1 is obliged to store such information as referred to in section 20 first paragraph 1 and 3 which is necessary to trace and identify the communication source, the destination of the communication, date, time and duration of the communication, type of communication, communication equipment and the location of mobile communication at the start and end of the communication.

> The retention requirement under the first paragraph includes data generated or processed in telephony, messaging, Internet access and the provision of capacity to get internet access (connection form). Even when a call is unsuccessful there is an obligation to retain data generated or processed.
>
> A person who is required to store the data under this section may instruct another person to carry out the storage.

The more detailed requirements are set out in the Ordinance (2003:396) on Electronic Communication (as amended by Ordinance 2012:128) – see also below.

There are provisions requiring communication providers to follow certain rules on interception capabilities in their networks. These are set out in administrative regulations from the Swedish body responsible for overseeing the ECA, the PTS (PTS regulation (2012:4)).

As regards norms which exist concerning the technical aspects of the internet providers' transfer of intercepted data to the police, e.g., with respect to formats and protocols, security measures and encryption, under section 37 of the Ordinance (2003:396) on Electronic Communication:

> Any entity which is required to store data according to ECA 6:16 shall take the measures necessary to ensure that the stored data is of the same quality and subject to the same level of safety and protection as was the case for the data before it was stored.
>
> The entity under the storage obligation shall take the necessary measures to protect the data against accidental or unlawful destruction and the accidental loss or alteration. Such measures should also be taken to prevent unauthorised storage, processing or access, and unauthorised disclosure of data. The data may be made available only to specially authorised personnel.

More detailed duties relating to physical and data security, together with encryption requirements are set out in PTS regulation (2012:4).

As regards norms regulating technical aspects of the internet provider's transfer of intercepted data to authorities in a foreign country (e.g., in the context of mutual legal assistance), the general rule in Swedish mutual legal assistance is that the same data is made available for foreign police, courts, and prosecutors as is available for their Swedish equivalents (Act on Mutual Legal Assistance (2000:562) 2:1). The same Act provides (4:25a) that direct transfer of data can occur to Iceland and Norway, if this can be done in a secure way. The same applies when Sweden is asked to assist technically another state to carry out an interception (4:25b). For EU states, direct transfer is possible under Chapter 3 section 34 of the Act (2017:1000) on a European Investigation Order. No special rules apply to technical aspects, meaning that what is available is only the same information available to the Swedish police/prosecutor, and only in the same form.

The telecommunications companies are to provide the requested data to the police, and this can presumably mean that the Security Police/police specify that only certain types of call are to be recorded. However, the Security Police/police do not usually wish to give away to the telecommunications company any operational details and so it is my understanding that the police do the necessary refining af-

terwards. A general duty to provide data in a usable form (meaning, *inter alia*, decrypted data) is to be found in ECA 6:19 which provides that "the provision of telecommunication services shall be conducted so that decisions on secret interception of electronic communications and covert surveillance of electronic communication can be executed […]. The content and information on intercepted or monitored communications must be made available in an easily accessible form."

5. Formal prerequisites of interception orders

The normal system is that the police, customs, or Security Police officer leading an investigation requests the prosecutor to bring an application before a court to approve telecommunications content interception. (CJP 27:21, para 1). In case of emergency, under CJP 27:21a (since 2014) it is provided that a prosecutor can give interim permission to intercept. The prosecutor must give reasons for his/her decision. If this emergency procedure is used, the case must immediately be brought before the responsible court which can confirm or terminate the interception order. This emergency procedure was previously only available under the 2008 Act, for listed security crimes, and was used rarely.[6]

The procedure is in writing. If the requesting prosecutor provides further oral information at the hearing, this must be documented. The court can request further information. It gives summary reasons for its decision. The application is a simple application before the court, not on oath. However, it is backed by the offence of misuse of office. In 2000, a prosecutor was convicted for having (negligently) applied for an interception warrant when the legal conditions were not fulfilled.[7]

6. Substantive prerequisites of interception orders

As regards the degree of suspicion for a past crime (or – in some countries – the degree of future danger or risk) necessary for an interception order, CJP 27:20 provides that: "Covert interception of electronic communications […] may only be conducted if someone is reasonably suspected of an offence […]."

Thus, reasonable suspicion of a specified, concrete, offence is necessary and there must normally be a suspected person. However, an amendment in 2012 now makes an exception to this rule, allowing interception of content in order to determine who may be reasonably suspected of a given, specific offence, where this is of particular importance to the investigation.[8] A legal person cannot commit an offence in Sweden, and so cannot be subject to an interception order.

---

[6] It was used four times between 2009–2012, see SOU 2012:44, p. 326.

[7] Lindberg, op. cit., p. 506.

[8] The text of the provision is set out above, section III.B.1. For the *travaux préparatoires* see Bill 2011/12:55, p. 130. Laxer requirements apply to the interception of traffic data, see below.

The normal use of coercive powers is only permissible to investigate an offence which has already been committed, is in the process of being committed, or in specific cases set out in law, where attempt, preparation, or conspiracy to commit an offence is punishable. However, proactive surveillance is now allowed under the Act (2007:979) on measures to prevent particularly serious crimes, when, having regard to the circumstances, there is reason to believe that a person will perform criminal acts in the future, including certain listed offences (such as sabotage, arson, terrorist offences, and murder). The 2007 Act moves the threshold for using interception of communications a little further forward in time for certain specified security-related offences. However, in practice the Act is not used much (not at all during 2014 or 2015). For particularly serious security-related offences, attempt, preparation, and conspiracy will also be punishable, and reach the statutory minimum sanction level for communications interception. Thus, where there are sufficient concrete indications to justify the application of the Act, there will almost invariably also be sufficient concrete indications to justify communications interception applying the normal rules in the CJP.

As regards which crimes or (dangers) can justify an interception order, CJP 27:18 provides that:

> Covert interception may be used in the preliminary investigation of: (1) offences punishable by a minimum period of two or more years' imprisonment; or (2) offences set out in section 2 para 2, points 2–7 (3) attempt, preparation, or conspiracy to commit such an offence if such act is subject to punishment (4) other offences if, with regard to the circumstances, it can be assumed that the punishment imposed will exceed more than two years imprisonment.

In Sweden, only serious offences are punishable by a minimum of two years imprisonment. Having said this, the effect of the Act on penalties for terrorist offences (2003:148), implementing the EU Framework Decision on Terrorism is that the commission of a list of ordinary offences with a terrorist intent carries a minimum penalty of four years imprisonment. Thus, if a terrorist intent is suspected, a long list of offences can form the basis of an interception order.

As regards (2), the list of crimes set out in section 2 para 2–7 are offences with a wide spectrum of penalties. In the circumstances, these offences will often fall under point (1) but not always (e.g., where a terrorist intent within the meaning of the above act is missing). These offences are:

1. sabotage or aggravated sabotage according to CC 13:4 or 13:5;
2. arson, aggravated arson, devastation endangering the public, hijacking, or maritime, aircraft or airport sabotage, according to CC 13:1, 2, 3, 5 a or 5 b, if the offence involves sabotage according to 13:4;
3. rebellion, armed threats against the lawful order or crime against civil liberty under CC 18:1, 3 or 5;
4. treason, inciting wars, espionage, aggravated espionage, unauthorised dealing with secret information, aggravated unauthorised dealing with secret information, or illegal intelligence activities against Sweden, against a foreign power, or against persons pursuant to CC19:1, 2, 5, 6, 7, 8, 10, 10 a or 10 b;

5. industrial espionage according to section 3 of the Act (1990:409) on the protection of business secrets, if there is reason to believe that the offence has been committed on behalf of or has been supported by a foreign power or by someone who has acted for a foreign power;
6. terrorist offences according to section 2 of the Act (2003:148) on penalties for terrorist offenses, offences under section 3 of the Act (2002:444) for the financing of particularly serious crimes in some cases, or offences under the Act (2010:299) on penalties for the public provocation, recruitment and training for terrorist offences and other particularly serious crime.

Point (4) is a "safety valve," introduced in 2004. It is mainly used for offences against property with a relatively wide sentencing scale.[9] It is stated in the *travaux préparatoires* that point (4) should be interpreted restrictively. It is only when there are good reasons for believing that the sentence will be more than two years imprisonment that the provision should be used as the basis for an interception order.

As regards who can be subject to an interception order (e.g., suspects, their intermediaries, their communication partners, specific devices), CJP 27:20 provides that:

> Covert interception of electronic communications and covert surveillance of electronic communications shall, unless otherwise provided in the second paragraph, only occur if someone is reasonably suspected of the offence and the measure is of particular importance to the investigation. This measure may only relate to 1. a phone number or address, or a certain electronic communication during the time of the authorisation which is held or has been held by the suspect or which may otherwise be assumed to have been used or may be used by the suspect, or 2. a phone number or address, or a certain electronic communication if there is particular reason to assume that the suspect during the time of the authorisation has or will contact this number etc.
>
> Secret surveillance of electronic communication shall, in addition to what is stated in the first paragraph, be carried out in order to investigate who may reasonably be suspected of the crime, if this is of particular importance to the investigation. However, only data relating to the past may be collected.

Thus, it is possible to monitor a teleaddress other than that held or used by the suspect if there are "particular reasons" to suspect that s/he will contact that number.

The targeting of particular communication content (e.g., through the automated use of certain trigger words) is only possible within the context of a signals intelligence operation by FRA directed against international communications.

There is no specific statutory requirement that the anticipated evidence will actually be obtained by means of the requested interception, however, as noted above, the measure must be of "particular importance to the investigation."

Nor is there a specific requirement that other – less intrusive – means of investigation must first be tried unsuccessfully or be considered unlikely to be successful. However, the application of the principles of proportionality and necessity will

---

[9] Lindberg, op. cit., p. 492.

often mean this in practice.[10] On the other hand, it is noted in the *travaux préparatoires* that it is not necessary first to have tried less intrusive means where it is obvious from the beginning that less intrusive measures will not be effective, or where this would involve the use of disproportionate police resources, would risk revealing the covert investigation or pose a risk to the lives of the investigators.

Interception must be proportionate to the seriousness of the offence in the individual case. The principle of proportionality has a special role in protecting the interests of third parties. These can sometimes be secured by attaching special conditions, e.g., real-time monitoring and the possibility of only recording communications where it is clear that the suspect is one of the parties. A duty to specify conditions designed to protect individuals' personal integrity is now an explicit part of CJP 27:21. As regards situations in which proportionality will be precluded, in the *travaux préparatoires* it is stated specifically that there is very little room for ever covertly intercepting the communications of a media company.[11]

According to the leading authority, an interception order should be required even when one of the parties to the communication has consented to the interception.[12] The police force in one region allegedly interpreted the law up until 2010 so as to permit them to use hidden microphones to record a conversation if one party to the conversation consented to this (i.e., wearing a wire). The case law of the European Court of Human Rights clearly requires court-ordered approval of this kind of coercive measure, and this was noted by the Commission of Inquiry on Certain Police Methods (SOU 2010:103). On balance, it should be assumed that this police practice is no longer followed.

7. Validity of interception orders

As already mentioned, the maximum length of an interception order under both normal circumstances and emergencies is one month. There is no limit set out in the law to prolongations, but the application of the principle of proportionality will often mean that limits will apply in practice. There were security cases in the 1960s when warrants were renewed every month for a period of 16 years. This would nowadays be regarded as quite unacceptable. However, security operations and organised crime investigations generally last longer than a month.

The renewal or prolongation of the interception warrant follows the same procedure as the initial application for an interception.

An interception order must be revoked when the circumstances show that it is no longer necessary. CJP 27:23 provides that "The prosecutor or the court shall imme-

---

[10] See Bill 1988/89:124, p. 66, Lindberg, op. cit., p. 501.

[11] See Bill 1988/89:124, p. 28.

[12] Lindberg, op. cit., pp. 53–54.

diately rescind an order authorising covert interception of electronic communications and covert surveillance of electronic communications once cause no longer exists for the order."

Interception does not need to be halted if it reveals information pointing to the commission of offences not anticipated by or not mentioned in the interception order. The issue of whether such information ("surplus information") may be used is now regulated in the law. CJP 27:23a provides that

> If, when covert interception of electronic communications […] has produced details of an offence other than that which has been the basis of the decision permitting the interception […] the resulting information may be used to investigate the offence in question if 1. imprisonment for one year or more is prescribed for the offence and it can be assumed that the offence does not result only in fines, or 2. there are special reasons for allowing this.

This provision was subject to considerable debate and only allowed after a detailed empirical study by a commission of inquiry (SOU 2012:44) revealed that there was no evidence that the police or prosecutor were deliberately circumventing the – relatively – demanding 2-year-minimum sentence rule by initiating investigations into more serious offence, in order to obtain information on less serious offences.

8. Recording, reporting, and destruction requirements

There are protocol duties which apply to the person leading the preliminary investigation under section 7 of the Ordinance on Preliminary Investigation (1947:948), as well as, for prosecutors, under internal regulations issued by the Prosecuting Authority. However, the protocol duties are kept separate from the preliminary investigation file. The practice is only to note covert interception or covert monitoring of traffic data in the preliminary investigation file if this is likely to be relied upon as evidence in a subsequent trial.[13]

There is no requirement that reports on progress of interception and final reports have to be submitted to the court. However, the interception period is relatively short, meaning that the authorisation must be renewed regularly and the prosecutor will be obliged to inform the court of any new relevant information and changed circumstances.

There are requirements to destroy the records which are not related to the aim of the interception warrant, or which are not needed as evidence. The prosecutor is responsible for these. The Commission on Security and Integrity Protection (SIN) has on occasion criticised prosecutors for not promptly ordering, and supervising, the destruction of records. New guidelines were therefore issued by the Chief Public Prosecutor in 2012.[14] SIN has also criticised the police for not promptly carrying out orders to destroy surplus information.

---

[13] Lindberg, op. cit., p. 515.

[14] ÅM RättsPM 2012:8.

9. Notification requirements and remedies against interception orders

There is a duty of the investigative authorities to inform intercepted persons about an interception. CJP 27:31 provides:

> Anyone who is or has been suspected of a crime shall, subject to section 33, notified of such covert interception or surveillance of electronic communications […] as he or she has been subjected to.
>
> If interception or surveillance of electronic communications has concerned a phone number or address, or certain electronic communication equipment possessed by someone other than the suspect, this person shall also be notified. This does not apply if the provisions of section 33 apply or it has taken place with the support of section 20, para 2 and the infringement of the individual's privacy is likely to be minor.
>
> […]
>
> A notification shall be submitted as soon as it can be without damaging the investigation, however, not later than one month after the investigation has been terminated.
>
> Notification need not be given to someone who already according to CJP 23:18 or otherwise has received access to the data. Notification is not required either if, with regard to the circumstances, it is obviously unnecessary.

CJP 27:32 provides

> Notification pursuant to section 31 shall include information on which coercive measure has been used and when it occurred. The person who is or has been suspected of an offence should obtain information about any suspected offence which has been the basis for the measure, or which the measure has led to. Anyone who is not, or has not been, suspected of an offence should be informed of this.
>
> A notice of covert interception of electronic communications or covert surveillance of electronic communications should also include a statement of which phone number or other address or which electronic communications equipment has been the subject of a warrant.

CJP 27:33 provides

> If secrecy applies under the Transparency and Secrecy Act (2009:400) 15:1 or 2, 18:1, 2 or 3 or 35:1 or 2, for information referred to in section 32, notification under section 31 may be postponed until the secrecy no longer applies.
>
> If one year elapses from the time of the completion of the investigation, and notification can still not be made because of secrecy requirements, the duty to notify expires.

The exception referred to in CJP 27:20, para 2 is for the relatively rare occasions when the police empty a mobile mast of metadata, in order to determine active mobile phones in the area (e.g., after a robbery).

The exceptions set out in Chapter 15 of the Transparency and Secrecy Act cover offences within the jurisdiction of the Security Police. Notification (almost) never occurs for these. Instead, the Commission on Security and Integrity Protection supervises all cases of non-notification.

The exceptions set out in Chapter 18 of the Transparency and Secrecy Act cover damage to ongoing criminal investigations. There is a specific exception in Chapter 18:17 covering mutual legal assistance.

The exceptions set out in Chapter 35 of the Transparency and Secrecy Act cover information potentially damaging to individuals' economic or personal integrity.

In theory: a person who receives notification can complain to the Commission on Security and Integrity Protection (SIN) and/or the chief government law officer (the Chancellor of Justice), or initiate a case before the civil courts (for damages). However, I know of no such cases since the late 1980s where this has occurred. There was a case concerning unlawful surveillance conducted by senior Security Police officers in the aftermath of the murder of Prime Minister Palme, where the people subjected to the unlawful surveillance attempted to secure full disclosure of methods, etc., and the prosecution demanded restrictions on the injured parties' right of access to the evidence. It is unclear how such a case would be resolved if it arose today. The Transparency and Secrecy Act applies, but so, too, does the right to a fair trial under IG and the ECHR. The issue has not been tested since the late 1980s and the situation is unclear.[15]

If SIN find that an offence (presumably misuse of office) has been committed in the course of surveillance operations it is to report this to the prosecutor with a view to prosecution. This has arisen only very rarely.

SIN is the independent monitoring authority which has the power to control, after the fact, the interception of communication and make sure that it is carried out in accordance with the legal requirements/legal authorisation. There were several reasons for creating SIN in 2007. Increased investigative powers had been, or were in the process of being, granted to the police and the Security Police. There was also a realisation that prosecutorial and judicial control only checked whether there was reasonable cause to initiate surveillance, and there was no *post hoc* monitoring. SIN was thus given a follow-up oversight function over surveillance. Having said this, the most important part of the work of SIN is still the function of monitoring personal data. SIN's mandate is 1) to ensure that surveillance activities by the police, and the Security Police, are conducted in accordance with laws and other regulations, and 2) that the police and the Security Police filing of personal data is "conducted in accordance with laws and other regulations." These laws include the limits set out on the filing of sensitive data in the Constitution (Instrument of Government Chapter 2 section 6; European Convention on Human Rights (ECHR) Article 8) and in the Police Data Act, as well as the police and the Security Police's own regulations on initiating, adding to, correcting, and terminating personal files. Although the mandate is only framed in terms of ensuring compliance with the law, a proportionality test is a fundamental part of this.

---

[15] Lindberg, op. cit., p. 512.

10. Confidentiality requirements on telecommunication providers and reliability requirements on those conducting telecommunication interceptions

There is a specific obligation for all service providers to keep their support measures confidential under ECA 6:20-23. Specific criminal sanctions for infringements of this obligation are set out in ECA 7:15, with a further reference to the CC (which in turn contains a reference to the content of a secrecy breach in the Act on Transparency and Secrecy).

There are also obligations for the person conducting the interception to maintain the integrity and reliability of the material obtained in CJP 27:24, and in Ordinance 1947:948. There is also a constitutional rule on impartiality and objectivity *(saklighet)* in IG 1:9.

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

In Sweden, law enforcement access to metadata is regulated in a number of different laws. The actual duty on service providers to retain the metadata for a period of six months is in the Act on Electronic Communication (2003:389), primarily in section 16a (see also below, regarding subscriber information).

Access by law enforcement to more extensive metadata than the name of a subscriber is regulated in the Act (2007:979) on measures to prevent particularly serious crimes, the Act (2008:854) on measures to investigate certain societally dangerous crimes and the Act (2012:278) on the collection of data on electronic communications in law enforcement intelligence. The 2007 Act is used relatively rarely. The 2008 Act provides for less stringent rules in certain circumstances for Security Police investigations into security crime but is not particularly significant in the area of metadata.

CJP section 19 provides

> Secret monitoring of electronic communication means that information is secretly gathered on
>
> 1. messages in an electronic communications which is or has been transferred to or from a phone number or other address, or
> 2. identifying which electronic communication equipment which has been present in a given geographical area, or
> 3. identifying the geographical area where specific electronic communications equipment has been present.
>
> Messages referred to in para 1 may also be prevented from reaching their destination through covert surveillance of electronic communications.
>
> Secret surveillance of electronic communication may be used during a preliminary investigation of

1. Offences for which the penalty is at least six months in prison,
2. Computer hacking under CC 4:9c, child pornography offences under CC 16:10a which are not regarded as minor, drug offences under section 1 of the Narcotics Act (1968:64), drug trafficking according to section 6 para 1 of the Act (2000:1225) on Penalties for Smuggling,
3. The offences referred to in section 2, para 2 p. 2-7, or
4. Attempts, preparation or conspiracy to commit an offence referred to in p. 1-3 above, if such an offence is punishable.

In the cases referred to in section 20 para 2, secret surveillance of electronic communications may be used only in preliminary investigations concerning offences that may lead to secret interception of electronic communications according to section 18 para 2.

Giving the police or Security Police access to metadata is not seen as a "coercive measure." However, it undoubtedly involves an interference with personal integrity within the meaning of the Swedish Constitution (above) and the ECHR. Because of this, access to metadata within the framework of a preliminary investigation requires court permission.

Although the main legal provision is in the CJP, the police and Security Police may, however, also access metadata if certain conditions are fulfilled, as part of their intelligence work under the above Act from 2012. The police and Security Police themselves decide whether or not to obtain this data, which can only be obtained if there is reasonable suspicion of "criminal activity" (but not sufficiently specified information so that one can say that they suspect that a particular criminal offence has been committed). Around 100 to 150 people are affected by such decisions taken by the police per year (SOU 2015:31, p. 263). The figure for the Security Police is not public, but probably double the figure for the open police (200 to 250 people). Some of these intelligence-based decisions later become preliminary investigations, and so there is overlap between these figures and those presented in the answer to question 2(a) above.

2. Use of traffic data and subscriber data

As regards the requirements for accessing traffic data in Sweden, to begin with, this is not yet possible by way of an automated online procedure. The Security Police have on several occasions requested telecommunications operators agree voluntarily to such a system, but this has been resisted. Competition is rife in the Swedish telecommunications market, and several Swedish companies, partly in order to attract and keep customers, advertise themselves as maintaining a high level of data integrity, i.e., keeping it secret even from the police.

Under CJP 27:20, a person must normally be reasonably suspected of the offence. However, a change was made in 2012, allowing access to metadata, but only historical (i.e., not real-time) data, in order to investigate who can be reasonably suspected of having committed the offence. In all cases, the measure must be of particular importance for the investigation before it can be ordered.

Under CJP 27:21 the court has to determine on the application of the prosecutor, whether the conditions required for the acquisition of metadata are met, the phone numbers and other addresses to be monitored, and the period of time for which access is granted, which may not exceed one month.

CJP 27:20 provides

> Covert interception of electronic communications and covert surveillance of electronic communications shall, unless otherwise provided in the second paragraph, only occur if someone is reasonably suspected of the offence and the measure is of particular importance to the investigation. This measure may only relate to
>
> 1. a phone number or address, or a certain electronic communication during the time of the authorisation which is held or has been held by the suspect or which may otherwise be assumed to have been used or may be used by the suspect, or
> 2. a phone number or address, or a certain electronic communication if there is particular reason to assume that the suspect during the time of the authorisation has or will contact this number, etc.
>
> Secret surveillance of electronic communication shall, in addition to what is stated in the first paragraph, be carried out in order to investigate who may reasonably be suspected of the crime, if this is of particular importance to the investigation. However, only data relating to the past may be collected.

The provisions in the CJP, especially after the changes made in 2012, would seem to cover all the conceivable situations when law enforcement need access to metadata. However, under the CJP, a preliminary investigation cannot be started to find out if an offence has been committed. Thus, police and Security Police investigations into organised crime and security crime respectively need some other legal basis. The 2012 Act regulates the preconditions for the police, the Security Police, and the Customs Service to collect metadata in the course of intelligence operations. Prior to the enactment of the Act, the agencies in question simply directed telecommunications providers to provide them with specified historical records.

The information which may be collected in accordance with section 1 of the Act is both historical traffic data (i.e., not real-time data) and location data – both historical location data and real-time location data. Data may be accessed if the circumstances are such that the measure is of particular importance to detect or prevent criminal activity involving crimes which have a minimum punishment of imprisonment for at least two years and if the measure is proportionate (section 2). Data may also be accessed where there is criminal activity involving certain specified security crimes which have a lower penalty than the minimum of two years (section 3). Generally speaking, Swedish sentences are relatively low, meaning that only serious offences are punishable by a minimum of two years. Thus, the threshold for intelligence access to metadata is set significantly higher than the threshold for access to metadata within the context of a preliminary investigation.

Decisions on whether or not to require production of metadata are made by the agency itself and are not subject to any prior external review (section 4). Formally

speaking, the head of the agency makes such decisions, but in practice this has been delegated down in the official hierarchy. However, no one actually participating in operational (intelligence gathering) activities is to take such a decision. Decisions shall be in writing, and the period covered by the order shall not exceed one month (section 5). If the metadata gathered indicates that criminal offences are being or have been committed, and the agency wishes to open a preliminary investigation, transfer of the metadata to the preliminary investigation requires court permission, applying the rules applicable for secret surveillance of electronic communications (section 8).

As regards the requirements for accessing subscriber data, the ECA provides for law enforcement access to information on who has a particular telephone number, or temporary IP address, *inter alia*, when this is necessary to investigate the commission of any offence. There is no requirement that the offence be punishable by a minimum sentence (unlike the case under the CJP or the 2012 Act). Minor offences can thus be investigated under the ECA, but only the name of the subscriber is available. This has, up to now, not been regarded as particularly serious from the perspective of personal integrity. As already mentioned, this is not possible by way of an automated online procedure.

Internet providers are required to retain subscriber information. Internet providers are also required to retain traffic data. The general duty of cooperation has already been mentioned. The more detailed requirements are set out in the Ordinance (2003:396) on Electronic Communication (as amended by Ordinance 2012:128). The relevant parts of this provide:

Section 39. In terms of telephony, the following are to be stored:

1. The caller,
2. The dialled number and the number that call is passed on to,
3. Information about the calling and the called subscriber and, where appropriate, registered users,
4. Date and traceable time when communication began, and ended, and
5. Details of the service or services that have been used.

Section 40. When it comes to telephone service over a mobile network access point, in addition to those mentioned in § 39, the following is to be stored:

1. The caller and the called subscriber's subscription identity and equipment identity;
2. The location information for the start and end of the communication, and
3. The date, traceable time and location data for the initial activation of a prepaid anonymous service.

Section 41. In terms of telephony service that uses IP packets for transmission, in addition to those mentioned in §§ 39 and 40, the following information is to be stored:

1. The caller and the called subscriber's IP addresses,
2. Date and traceable time for log-on and log-off or the services used, and
3. Information identifying the equipment where the communication between the entity with the storage obligation and the individual subscriber is completed.

If the entity which finally relays the communication to the individual subscriber is not covered by ECA 6:16 a, the first paragraph 3 applies to the entity which relayed the communication to that entity.

Section 42. In terms of messaging, the following are to be stored:

1. Sender's and recipient's number, IP address, or other communication address,
2. Information on sending and receiving subscriber and, where appropriate, registered users,
3. Date and traceable time for log-on and log-off or the services used,
4. Date and traceable time of dispatch and receipt of message, and
5. Details of the service or services that have been used.

Section 43. In terms of internet access and the provision of capacity to obtain internet access (connection form) the following should be stored:

1. The user's IP address,
2. Information on the subscriber and, where applicable, registered users,
3. Date and traceable time for log-on and log-off service providing Internet access;
4. The type of transmission capacity used, and
5. Information identifying the equipment where the communication between the entity with the storage obligation and the individual subscriber is completed.

If the entity which finally relays the communication to the individual subscriber is not covered by ECA 6:16 a, the first paragraph 5 applies to the entity which relayed the communication to that entity.

All the above data is to be made available on request to law enforcement agencies. Failure to do so is sanctioned by the PTS through administrative fines. It should be noted that after the Court of Justice of the EU (CJEU) declared the Data Retention Directive null and void, certain telecommunications companies refused to hand over data on request in cases where the police or Security Police requested this for intelligence operations under the 2012 Act (as opposed to a preliminary investigation into an offence, which had been authorised by a court). The PTS was unsure of whether the Swedish 2012 Act was in compliance with the CJEU's judgment and announced that, pending clarification, it would not enforce the duty to cooperate by issuing administrative fines. A commission of inquiry was appointed which analysed the judgment. It came to the conclusion that the 2012 Act (which, *inter alia*, provides for *post hoc* control by SIN) set out sufficient safeguards to be in compliance with the requirements of EU law (as clarified by the CJEU).[16] The PTS then resumed sanctioning non-compliance, and the telecom companies resumed their compliance. However, two telecom companies appealed the PTS decision. The district administrative court ruled against them, whereupon this in turn was appealed. The administrative court of appeal has recently requested a preliminary ruling from the CJEU on whether the Swedish system is in compliance with EU law or not. In the meantime, one of these companies has refused to

[16] Ds. 2014:23. A later, follow-up, inquiry made a detailed empirical study of police and Security Police use of metadata under the 2012 Act and came to the same conclusion. See SOU 2015:31.

comply with police orders to produce traffic data for intelligence purposes, and is facing administrative fines.[17]

3. Identification of the device ID (IMEI) and location of mobile terminal devices

The device ID (IMEI) is part of the information which must be stored and made available by the service provider. IMSI catchers are also in use in Sweden, although their use is apparently rare. This is not specifically regulated, apparently on the basis that this is not a significant infringement on privacy (IG 2:6 para 2 above). This is not a strong argument, but in any event, the failure to regulate specifically the use of IMSI catchers means that their use will probably violate Article 8 ECHR.

D. Access to (Temporarily) Stored Communication Data

Access to (temporarily) stored communication data is possible for messages which have been delivered to the recipient and so stored in his/her mobile or computer.[18] This is not possible for data in the possession of the ISP. Instead, a warrant has to be issued for interception of electronic communications. Access to stored communication may thus only be performed as an open measure, not in a clandestine way. As noted above (III.B.3.), a legislative proposal will be introduced in 2019 providing for hacking. However, it is likely that this will exclude the clandestine accessing of stored communications in the possession of the ISP.

The principle of proportionality applies to seizure. This standard of proof means that there must be specific evidence of specific strength indicating that the property is of importance for the investigation of the offence.[19] The Chancellor of Justice and the Ombudsman have on occasion criticised the police and prosecutors for seizing a person or a company's computers – making their continued business activity impossible. The police and prosecutors have therefore adopted a more restrictive approach, copying data which is then destroyed to the extent it is not necessary

---

[17] For more discussion, see Cameron, I., Law enforcement access to metadata in Sweden, in Lind, A. S., Reichel, J., Österdahl I. (eds), *Information and Law in Transition*, Liber, 2015. The Advocate-General's opinion in Joined Cases C-203/15 *Tele2 Sverige AB v. Post-och telestyrelsen* and C-698/15 Secretary of State for Home Affairs was published on 16 July 2016. Basically the Advocate-General considers that a general requirement of data retention is compatible with EU law, but that each of the safeguards set out by the ECJ in the Digital Rights Case must be satisfied (instead of making a general appraisal of the national system of safeguards as a whole). If upheld by the ECJ, this would mean making a change to the law, introducing a requirement of prior judicial or quasi-judicial approval before the police or Security Police may access metadata for intelligence purposes.

[18] SOU 1998:46, p. 373; Lindberg, op. cit., p. 522.

[19] See, e.g., SOU 2011:45, p. 274; Lindberg, op. cit., p. 45.

for the investigation. There is, on the other hand, a greater degree of latitude given when transferring such data abroad in execution of a request for mutual legal assistance.[20]

As regards the issue of cooperation duties for decoding encrypted data, in Sweden a witness can be obliged to witness under oath in court proceedings, but there is no possibility for the police or a prosecutor to insist that a suspect hand over a password.

IV. Use of Electronic Communication Data in Judicial Proceedings

As regards the issue whether there are specific rules for using intercepted electronic communication data in criminal procedure, Swedish procedural law is based on the principle of free evaluation and admissibility of evidence. It is the court which determines the value to be given to a particular piece of evidence, for example, a conviction could be based purely on circumstantial evidence.

Intercepted material can be introduced as evidence in criminal proceedings in the form of transcripts, audio recordings, and witness testimony. The principle of orality means that witness testimony is the primary method. Transcripts and the original recordings can be used if for some reason witness testimony is not available or if it assists the court in understanding the evidence.

Evidence which has been obtained in a fashion which is regarded as improper, or where the rights of the defence have not been properly safeguarded, is still admissible but will usually be given a low or very low evidential value. In a case where the court considers that the police have acted through an *agent provacteur*, the court will apply ECtHR case law and disregard the evidence.

As noted above, intercepted data can be used for the prosecution of offences other than the offences mentioned or anticipated in the interception order. Moreover, intercepted data can be used for the prosecution of individuals who were not the subject of the underlying interception order, so long as the (relatively strict) conditions for use of surplus information are met.

Intercepted data obtained from outside the criminal justice system (e.g., intelligence services, non-judicial police forces) is at the present time not admissible as evidence in criminal proceedings. However, there has been a recent proposal by a commission of inquiry (SOU 2015:163) that it should be possible for the signals intelligence agency (FRA) to continue to monitor communications of suspected "foreign fighters" and collect, on behalf of the Security Police, evidence that these

---

[20] See NJA 2013, s. 867 below.

people have committed offences. However, this evidence would not be directly admissible in subsequent trials. This proposal has been criticised, and it is unclear whether it will result in a legislative bill.

As far as transnational criminality is concerned, the principle of free admissibility of evidence means that evidence gathered by foreign police and prosecutors, in whatever form, can be presented. Nor is it essential that foreign witnesses physically attend the main hearing in Sweden. Although efforts are invariably made to allow such witnesses to give their evidence by means of live telephone or video links, where this is impracticable, written statements are usually admissible.

As regards the possibilities the accused has of challenging the probity of intercepted evidence, when a preliminary investigation has reached the point where a person is reasonably suspected of a crime, s/he should be informed of these suspicions (they will usually have been charged and arrested at this point anyway). There are two schools of thought as to whether such a suspect has the right to be informed of the results of the preliminary investigation. When a person has been formally accused of the offence (which usually occurs at the time of trial), it is clear that s/he has the right under CJP to be informed) of all relevant evidence and have access to the material gathered in the preliminary investigation. If this is refused, s/he can apply to the court to grant him/her access. Where a preliminary investigation is discontinued without leading to a formal accusation and trial, the person previously suspected has no explicit right to receive the preliminary investigation file. However, refusal to grant access to the file can be appealed to the administrative courts, and the Supreme Administrative Court has on occasion found that the person's interests in seeing the file outweigh the interests involved in keeping it secret. So far, none of these cases have involved covert surveillance.[21]

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

Mutual legal assistance is governed generally by the Act on International Legal Assistance (2000:562).[22] However, for EU states (apart from Denmark and Ireland) the main statute is now the Act (2017:1000) on a European Investigation Order which displaces the Act on International Legal Assistance, to the extent that there is

---

[21] Lindberg, op. cit., p. 513.

[22] For more discussion, see Cameron, I., Schunke, M. Påle-Bartes, K., Wong, K. and Asp, P., *International Criminal Law from Swedish Perspective*, Intersentia, Brussels, 2011, chapter 4.

overlap.[23] For non-EU states, Denmark and Ireland, the Act on International Legal Assistance can form the basis of granting requests from other states, i.e., Sweden does not require that another state requesting mutual legal assistance has acceded to a treaty to which Sweden has also acceded. However, accession to such a treaty generally makes the provision of mutual legal assistance easier. Sweden has acceded to the following most central multilateral conventions concerning international legal assistance in criminal matters:

1. the European Convention (1959) on Mutual Assistance in Criminal Matters (hereafter the "ECMLA"), including the two additional protocols of 1978 and 2001,[24]
2. the European Convention (1977) on Terrorism,[25]
3. the United Nations Convention (1988) against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,[26]
4. the European Convention (1990) on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime,[27]
5. the Schengen Convention (1990),[28]
6. the United Nations Convention (2000) against Transnational Organized Crime and its supplementing Protocols,[29]
7. the European Convention (2000) on Mutual Assistance in Criminal Matters (hereafter "EUCMLA"), and its Protocol of 16 October 2001,[30]
8. the international Agreement of 19 December 2003 between the EU and Norway and Iceland.[31]

Apart from these most central conventions, Sweden has also ratified other treaties which are not primarily regulating international cooperation in criminal matters but still contain clauses on mutual assistance. Sweden also has a small number of bilateral treaties with states (e.g., with China, regarding Hong Kong). Sweden has signed, but not yet ratified the Convention on Cybercrime.

---

[23] See Act on International Legal Assistance, section 7a, Prop. 2016/17: 218.

[24] SÖ 1968:15, SÖ 1979:12 and Bills 1961:48 and 1978/79:80. The second additional protocol to the ECMLA has not yet been ratified by Sweden. However, most of the provisions of this protocol are already implemented into Swedish law mainly through the implementation of the EUCMLA 2000 and its Protocol of 16 October 2001.

[25] SÖ 1977:12 and Bill 1976/77:124.

[26] SÖ 1991:41 and Bill 1990/91:127.

[27] SÖ 1996:19 and Bill 1995/96:49. The Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, ETS 198, has been signed but not ratified by Sweden.

[28] SÖ 1998:49 and Bills 1997/98:42, 1997/98:58 and 1999/2000:61.

[29] SÖ 2004:21 and Bills 2002/03:146, 2003/04:111 and 2004/05:138.

[30] SÖ 2005:42, SÖ 2005:43 and Bill 2004/05:144.

[31] OJ L 26, 29.1.2004, p. 1 and Bill 2004/05:144.

As regards guidelines for the competent authorities regarding the cross-border interception of telecommunications, there are two general handbooks for prosecutors published by the Prosecution Authority, one dealing with the European Investigation Order, and one dealing with the Act on International Legal Assistance.[32]

B. Procedures and Execution of Requests

There are no special prerequisites concerning requests for interception of telecommunications in the Swedish Acts on International Legal Assistance and on a European Investigation Order. The rules in the CJP are applicable also when the measures are taken upon request from a foreign state. As the Act on a European Investigation Order is based on mutual recognition, the Act provides for a number of obligatory or optional grounds for refusing foreign requests, national security, *ne bis in idem*, etc. (Chapter 3 sections 5 and 6). All these grounds are set out in the Directive: no additional grounds are provided for.

Foreign requests for interception of telecommunications are handled by the responsible prosecutor (who will often be attached to one of the three specialist international prosecution chambers). The prosecutor shall immediately consider if the prerequisites for the measure exist and in such a case apply to the court for permission to undertake the measure.[33]

Where a Swedish prosecutor has sought covert electronic interception or surveillance, s/he must apply the CJP rules on legal privilege to the data delivered and filter out or delete information which would have been privileged had it been gathered in Sweden.

A request to execute a cross-border interception of a person present in Sweden (or rather, a telecommunications address held or used in Sweden)[34] may only be made from an EU Member State or from Iceland or Norway and must concern a criminal investigation.[35]

The prerequisites for Swedish authorities to give consent to a foreign cross-border interception of telecommunications are identical to those which rule requests for the traditional forms of interception.[36] These stricter conditions, for example, concerning the minimum penalty applicable to an offence before interception can be ordered, are due to the fact that the address to be intercepted in such a case is held or used in Sweden. Even though Sweden is in general positive to ju-

---

[32] Published by the section for international legal assistance, in respectively, 2001 (with updates) and December 2017.

[33] Ch. 4 sec. 25 para 1 ILA Act.

[34] See Bill 2004/05:144 p. 206.

[35] Ch. 4 sec. 26a para 1 ILA Act.

[36] Ch. 4 sec. 26a para 3 ILA Act.

dicial cooperation based on the principle of mutual recognition, execution of decisions involving telecommunications interception is particularly sensitive.[37] There is a requirement of double criminality. Requests are handled by a prosecutor, who shall immediately consider if the prerequisites for the measure exist, and in such a case apply to the court for permission to undertake the measure.[38] Having set out the conditions, it is unclear if this measure is used in practice. The long land borders with Norway and Finland would indicate that there will be some situations in which these states might be able to intercept telecommunications in Sweden near the border. Separate statistics on this are, however, not available in Sweden.

Swedish communication providers are under a duty of confidentiality, which can only be waived in relation to Swedish police, prosecutors, and courts: thus requests must go through the Swedish system.

In my opinion, relatively few technical, legal, and organisational national reform measures would be necessary to enable "real time cooperation" in the field of interception measures or to increase its effectiveness, assuming there is mutual trust. This undoubtedly exists as regards other Nordic states and some EU states (including Germany), but almost certainly not for others. If such a possibility were introduced as a result of an EU measure, implemented into Swedish law, the likelihood is that Sweden, during the negotiations, would probably want to make it discretionary, rather than mandatory. Moreover, it is likely that it would be limited by reference to safeguards which could be adapted to fit individual cases, depending upon which EU state had requested the data etc.

C. Statistics

International requests make up a small proportion of the whole: in 2007 these amounted to 42 of 996 warrants issued, in 2008, they were 28 of 990 issued.[39]

According to more recent figures, in 2013, 72 applications were made on behalf of foreign states and granted for covert interception of electronic communications.[40] In 2014 and 2015, the figure was 84 applications made and granted. In 2016, the figure was 78 applications made and granted. In 2017, the figure was 49 applications made and granted. Many of these concerned the same person(s), i.e., permission was extended for several periods of one month. In 2014, a total of 39 people were affected by these applications, in 2015, 13 people, in 2016, 29 people, and in 2017, 16 people.

---

[37] See Bill 2004/05:144 pp. 178–179.

[38] Ch. 4 sec. 26a para 1–2 ILA Act.

[39] See respectively Rskr 2008/09:79, p. 16 and Rskr. 2009/10:66, p. 8. A warrant can involve more than one teleaddress and can therefore concern more than one person.

[40] Figures from 2013–2017 come from ÅM 2017/2170.

In 2013, 245 applications were made on behalf of foreign states and granted for covert surveillance of electronic communications. In 2014, the figures were 204 applications made and granted. In 2015, the figures were 161 applications made and 160 granted. In 2016, the figures were 209 applications made and 208 granted. In 2017, the figures were 103 applications made and granted. Again, many of these concerned the same person(s), i.e., permission was extended for several periods of one month. In 2014, 85 people were affected, in 2015, 63 people, in 2016, 76 people, and in 2017, 28 people.

Figures broken down by country are not available, however on the basis of questions put to the relevant prosecutors, a small proportion of these concerned requests from Germany.Bibliography

Bibliography

Lindberg, G., *Straffprocessuella Tvångsmedel* (Coercive measures under the law of criminal procedure), 4 uppl. Karnov, 2018.

Lind, A.S./Reichel, J./Österdahl I. (eds.), *Information and Law in Transition.* Liber, 2015.

Cameron, I./Schunke, M./Påle-Bartes, K./Wong, K./Asp, P., *International Criminal Law from Swedish Perspective*. Intersentia, Brussels, 2011.

List of Abbreviations

CJP	Code of Judicial Procedure
Ds	Departmental commissions of inquiry
ECA	Electronic Communications Act
ECHR	European Convention on Human Rights
ECJ	Court of Justice of the European Union
ECMLA	European Convention (1959) on Mutual Legal Assistance in Criminal Matters
ECtHR	European Court of Human Rights
EUCMLA	European Convention (2000) on Mutual Legal Assistance in Criminal Matters
FRA	Defence Radio Establishment
IG	Instrument of Government
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISP	Intelligence and Security Service
NJA	Supreme Court reports

PTS	Post and Telecom Authority
Rskr	Government report to parliament
SIN	Commission on Security and Integrity Protection
SIUN	Defence Intelligence Inspection
SÖ	Swedish treaty series
SOU	State Commissions of Inquiry

The United Kingdom*

National Rapporteur:
Elif Mendos Kuskonmaz

* This report outlines the legislation and case law as of October 2018. The author is grateful to Prof. Ian Walden for his helpful feedback on the earlier draft of this report.

Contents

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Security Services with Powers of Telecommunication Interception

1. National security architecture

In the UK, the key agencies responsible for national security are the Security Services (MI5) and the Secret Intelligence Services (MI6). The former has responsibility for domestic counter-intelligence, whilst the latter is responsible for foreign intelligence. The existence of MI5 was avowed by the government through the Security Service Act (SSA) 1989 and MI6 by the Intelligence Services Act (ISA) 1994. Both services have the functions of protecting national security, safeguarding the 'economic wellbeing of the United Kingdom' and 'the detection and prevention of serious crime.'[1] The agencies are supported by the Government Communications Headquarters (GCHQ), which provides signals intelligence. Within the Ministry of Defence, there is also Defence Intelligence, providing strategic defence intelligence to the Ministry and the armed forces.

The police are primarily responsible for criminal law enforcement. The structure of the UK police can be sub-divided into national and territorial bodies, the latter reflecting the different regions within England, Scotland, Wales and Northern Ireland. In addition to the police, the UK has the National Crime Agency (NCA) with responsibility for tackling serious and organised crime through its 'crime reduction function' and its 'criminal intelligence function.'[2] The NCA is a non-ministerial government department, rather than a policing agency, and was established in 2013. Its remit includes the National Cyber Crime Unit.

2. Powers for the interception of telecommunication

The Investigatory Powers Act (IPA) 2016 is the main legal basis for the rules on electronic communication interception and other covert investigatory measures; these are the acquisition of communications data, retention of communication data, equipment interference, bulk acquisition of communications data, and bulk equipment interference. It brings together the regime under which both UK law enforcement and intelligence agencies can conduct all the above covert investigatory measures. It received the Royal Assent on 29 November 2016, but it is only partly implemented and the date of its full implementation is uncertain. Following the

---

[1] Security Service Act 1989 (SSA), s. 1 and Intelligence Services Act 1994 (ISA), s. 1.

[2] Crime and Courts Act 2013, s 1.

decision by the UK High Court on April 2018 on the incompatibility of the communications data retention provisions of the IPA 2016 with EU law, the UK Government proposed some changes to make the IPA 2016 EU-law complaint.[3] Those changes are contained in the Data Retention and Acquisition Regulations 2018, which entered into force in October 2018. The changes that they bring include restricting purposes for which authorities may request access to certain communications data to the purpose of prevention or detection serious crime and providing a new threshold of 'serious crime,' which includes the imprisonment for a term of 12 months (as opposed to the imprisonment for a term of 3 years or more in the earlier version of the IPA 2016).

The IPA 2016 contains two different interception regimes; one relates to targeted interception and the other relates to bulk interception. The former regime contains rules on intercepting communications, via telecommunication systems or postal services, for law enforcement purposes (s. 15) both by law enforcement and intelligence authorities. This interception can be carried out in a thematic way (i.e., targeted thematic interception) whereby interception does not relate to a single person or set of premises, but relates to 'a group of persons who share a common purpose or who carry on, or may carry on a particular activity' or to more than one person, organization, or set of premises where the interception is requested 'for the purposes of a single investigation or operation' (s. 17(2)). The Act also provides rules for intercepting overseas-related communication in bulk (i.e., bulk interception) for intelligence purposes by intelligence agencies (Part 6 Chapter 1). As discussed further below, the purposes for which an interception can be carried out, the context of such interception, and the authorities that can request the interception differ under the regimes of targeted and bulk interception.[4] The IPA 2016 is supplemented by regulations and codes of practice that detail the covert investigatory measures provided by it.

There are also other covert investigatory measures under different statutes. The Regulation of Investigatory Powers Act (RIPA) 2000 contains provisions on the authorisation of surveillance and covert intelligence resources (Part II).[5] The Police Act 1997 and the ISA 1994 provide the rules on property interference by the law enforcement and intelligence agencies.

3. Responsibility for the technical performance of interception measures

The technical implementation of all interception measures rests upon the telecommunications service operator. The targeted interception warrant cannot require the operator to do things that are not 'reasonably practicable' (s. 43(4)). Neverthe-

---

[3] [2018] EWHC 975.

[4] Section III.C.1.

[5] Section III.C.2.

less, the operator can be served a technical capability notice issued under the IPA 2016 in order to ensure that it has the capacity to assist with an interception warrant (s. 253 IPA 2016 and Investigatory Powers (Technical Capability) Regulations 2018). Thus if an operator is served with a technical capability notice, the extent of the practicability of the assistance required under the interception warrant is to be examined on the basis of the compliance of the operator with that notice (s. 43(6)). The rules on the reasonable practicality and the technical capability notice apply in relation to the bulk interception measures as they apply to the targeted interception measures (s. 149(5)).

The IPA 2016 covers non-UK based telecommunication operators if they provide telecommunications services to people in the UK or control a telecommunication system in the UK (s. 261(10)). Therefore, these operators have the duty to provide all assistance in giving effect to interception measures. However, they can raise the defence that they are not required to take steps in pursuance of interception measures because they are in breach of any requirements or restrictions under the law of the country where they are based (ss. 43(5) and 149(5)). Similarly to UK based operators, non-UK based ones can be subjected to technical capability notices, obliging them to provide capabilities to assist with interception (s. 253(8)). A centralized institution, the National Technical Assistance Centre (NTAC), which is part of GCHQ, provides technical assistance for law enforcement and intelligence agencies in interception.

4. Legitimacy of data transfers between different security agencies

The law enforcement and intelligence agencies regularly perform joint operations. For example, the GCHQ and the NCA work together in tackling serious and organized crime. Also, the intelligence agencies may have statutory obligations to aid law enforcement agencies. For example, one of the statutory functions of MI5 is to assist law enforcement agencies in the prevention and detection of serious crime (s. 1(4) Security Service Act 1989).

The results of interception measures can be shared between different competent authorities within the UK subject to safeguards regarding disclosure of the warrant (s. 53 IPA 2016 for targeted interception warrants, and s. 130 IPA 2016 for bulk interception warrants). A law enforcement agency may ask an intelligence agency to share information obtained under a bulk interception warrant under two conditions. The first condition is that the law enforcement agency must have exhausted all other means of progressing the operation or investigation. The second condition is that the request for information sharing must be necessary and proportionate. In such a case, the intelligence agency may provide assistance to the law enforcement agency if the latter provides supporting material sufficient for the former to determine the necessity and proportionality of the information sharing and safeguards in

relation to the examination, retention, and disclosure of material obtained under the bulk interception warrant are met.[6]

Material obtained through targeted or bulk interception can be exchanged with other countries, in particular with their intelligence agencies. The legitimacy of this exchange in light of the European Convention on Human Rights (ECHR) was confirmed by the European Court of Human Rights (ECtHR) in its *Big Brother Watch* decision on 13 September 2018.[7] The IPA 2016 provides certain conditions for such an exchange to take place. Accordingly, for material obtained through targeted interception to be shared with an overseas authority, the Secretary of State must be satisfied that safeguards in relation to retention and disclosure of material are in place to the extent that he or she finds appropriate (s. 54(2)(a)). Also, because the intercepted material is inadmissible before the UK courts, the Secretary of State must be satisfied that restrictions are in place that would prevent, to the extent that he or she thinks appropriate, the disclosure of the material in legal proceedings outside the UK (s. 54(2)(b)). For material obtained through bulk interception, the Secretary of State must be satisfied that safeguards relating to minimising the disclosure, copy, distribution, retention, examination of content or secondary data are in place to the extent he or she considers appropriate (s. 151(2)(a)). Also, restrictions on the disclosure of the material in legal proceedings outside the UK are sought, similarly to restrictions in relation to the material obtained through targeted interception (s. 151(2)(b)).

According to the Interception of Communications Code of Practice, these conditions will be considered to be satisfied for the long established intelligence sharing relationships of the UK (e.g., Five Eyes).[8] Where the information needs to be shared with a country with whom the UK does not have an existing relationship and which does not have similar safeguards as afforded under the IPA 2016, the person considering the authorisation for the sharing of information must balance the risk that subjecting the material to a lower level of safeguard may entail against a risk to national security stemming from the non-disclosure.[9]

B. Statistics on Telecommunication Interception

The intercepting authorities must keep the statistics on their application for the issuance of interception warrants (targeted or bulk) in order to aid the IPC in performing its oversight duties.[10] Under the IPA 2016, the statistics on interception

---

6 Interception of Communications Code of Practice, paras. 9.16–9.18.

7 *Big Brother and others v United Kingdom* [2018] ECHR 722.

8 Interception of Communications Code of Practice, para. 9.28.

9 Ibid., para. 9.29.

10 Section III.B.8.

measures must be reported annually to the Prime Minister by the Investigatory Powers Commissioner (IPC) (s. 234(1)). It must also make reports to the Prime Minister upon their request at any time (s. 234(3)). Both types of reports must be brought before the UK Parliament (s. 234(6)) As the IPC only assumed its role in March 2017, the statistics on covert investigatory powers can be found in the annual reports made by its precursors; namely the Interception of Communications Commissioner's Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (ISC). According to the IOCCO, the number of interception warrants issued over the last 5 years is as follows:[11]

Year	Number
2016	3007
2015	3059
2014	2795
2013	2760
2012	3372

It is important to note that the above statistics relate to interception warrants authorised under the RIPA 2000, the predecessor of the interception regime under the IPA 2016.

According to the ISC, the number of warrants and authorisations issued in accordance with the RIPA 2000 and the ISA 1994 for the last 5 years is as follows:[12]

Year	Number
2016	1926
2015	1560
2014	2032
2013	1887
2012	2838

[11] IPCO, Publications, IOCCO Publications available at https://www.ipco.org.uk/default.aspx? mid=14.12.

[12] IPCO, Publications, ISC Publications available at https://www.ipco.org.uk/default.aspx?mid=15.13.

II. Principles of Telecommunication Interception in Constitutional and Criminal Procedural Law

A. Constitutional Safeguards of Telecommunication

1. Areas of constitutional protection

The UK does not have a written constitution, but the Human Rights Act 1998 gives domestic effect to the human rights enshrined in the ECHR (e.g., Article 8 on the right to respect for private life) as interpreted by the ECtHR. Therefore, the HRA compels compliance by public authorities with the ECHR's human rights standards. The ECtHR has on several occasions contemplated the legality of the UK law on interception of both domestic and external communications.[13]

Another human rights protection comes from the EU Charter of Fundamental Rights (Charter) to the extent that the UK acts within the scope of EU law. Therefore, Articles 7 (right to respect for private and family life) and 8 (right to protection of personal data) of the Charter provide protection for individuals against interception measures. However, the UK voted to withdraw from EU membership and the exit is due to take place on 29 March 2019. The EU (Withdrawal) Act 2016, which repealed the legislation that brought the UK into the EU (i.e., the European Communities Act 1972), states that the Charter will not be part of the UK law once the UK exits the EU (s. 5(4) of the EU (Withdrawal) Act 2016). Therefore, Article 8 of the Charter, which is not explicitly part of the ECHR, will cease to be an enforceable right under domestic law after the UK's exit from the EU.

2. Proportionality of access to data

The principles of proportionality and necessity are applicable when determining the compliance of a measure with the human rights standards of the ECHR and the Charter. The IPA 2016 explicitly mentions the proportionality and necessity requirements. For example, the Secretary of State can issue a warrant for an interception (targeted or bulk) after evaluating the proportionality and necessity of that interception in relation to the objective pursued by the warrant (ss. 19(2) and 102(3)).

3. Consequences for the interception of telecommunication

Under the IPA 2016, the criminal offences of illegal interception and unauthorised obtaining of communications data carry up to two years of imprisonment or a fine on indictment (s. 3(6)). The monetary penalty for illegal interception must not

---

[13] *Malone v United Kingdom* [1984] 7 EHRR 14; *Halford v United Kingdom* (1997) IRLR 471; *Liberty and others v United Kingdom* [2008] ECHR 568; *Kennedy v United Kingdom* [2010] ECHR 682; *Big Brother and others v United Kingdom* [2018] ECHR 722.

exceed £50,000 (s. 7(5)). Breach of the safeguards by the intercepting authority in relation to the protection of the use of intercepted material and the restriction on certain types of communications however, does not give rise to criminal or civil liability.

According to the Computer Misuse Act (CMA) 1990, s. 1 and s. 3 offences carry the maximum penalty of two and ten years' imprisonment, respectively.

Also, the criminal offence of unlawful obtaining of personal data under the Data Protection Act (DPA) 2018 carries maximum £50,000 fine (s. 196(2)). Breach of obligations set out under the DPA 2018 can lead to administrative fines (s. 157). For example, failure to comply with the basic data protection principles for processing of personal data carries a fine of up to 20 million Euros or 4% of the total worldwide annual turnover, whichever is higher.

4. Statutory protection of personal data

There are several statutory safeguards for the protection of secrecy of telecommunication that can trigger criminal, civil, or administrative law remedies if breached. The IPA 2016 establishes criminal liability for illegal interceptions (s. 3(6)), imposes monetary penalties (s. 7), and creates a statutory tort (s. 8). It also criminalises the unauthorised obtaining of communications data (s. 11). Moreover, the IPA 2016 provides further safeguards for the protection of the secrecy of communications. It provides safeguards for the use of intercepted material such as limiting the number of authorities to whom the material can be disclosed and the extent of such disclosure to a minimum that is necessary for the authorised purpose of interception (ss. 53(2)–(3) IPA 2016), storing the material in a secure manner (s. 53(4)), and destroying it as soon as there are no legal grounds for retaining it (s. 53(5)). Also, the IPA 2016 introduces specific restrictions on the implementation of (targeted) interception measures concerning Members of Parliament, items subject to legal professional privilege, confidential journalistic material, and sources of journalistic information (ss. 26–29).

The CMA 1990 also criminalises the unauthorised access of computer material (s. 1) and unauthorised access with intent to impair the operation of a computer (s. 3). These offences may be invoked in relation to unauthorised interception in the course of a transmission. However, enforcement officers acting in relation to powers of inspection, search, or seizure are immune from liability (s. 10).

Other criminal liabilities that can be relevant in relation to the protection of the secrecy of telecommunications can be found under the Data Protection Act 2018. This Act supplements the EU General Data Protection Regulation (GDPR) by regulating the data protection derogations under the GDPR and by covering areas that are excluded from it (e.g., national security matters) and transposes the EU Law

Enforcement Directive. The DPA 2018 criminalises unlawful obtaining of personal data (s. 170).

B. Powers in the Code of Criminal Procedure

The UK does not have a single written criminal code, but the principle of legality is a vital condition of the rule of law that is one of the key principles of the UK constitution. The general powers of police to investigate crimes derive from the Police Act 1997 and the intelligence authorities derive their powers from the SSA 1989 and the ISA 1994.[14]

III. Powers for Accessing Telecommunication Data in the Law of Criminal Procedure

A. Overview

The IPA 2016 contains several powers granted to law enforcement and intelligence authorities in intercepting and accessing electronic communications.

- Part 2, Chapter 1 governs the interception of communications content in the course of its transmission.
- Part 3 concerns the acquisition of communications data, which is the information about communications (i.e., who, where, when, what, and how).
- Part 4 relates to the retention of communications data whereby telecommunications operators are obliged to retain communications data for a certain period to enable access to this data for law enforcement and intelligence agencies.
- Part 5 addresses equipment interference whereby law enforcement or intelligence agencies access a device, system, or network.
- Part 6, Chapter 1 governs the rules on bulk interception allowing intelligence agencies to obtain foreign-focused intelligence and to later examine it.
- Part 6, Chapter 2 provides rules for bulk acquisition that covers the acquisition of communications data by intelligence agencies without a defined target.
- Part 6, Chapter 3 contains the requirements for bulk equipment interference that can be sought exclusively by the SIA for interfering with computers with a foreign focus.
- Part 7 relates to the SIA's power of retaining bulk personal datasets, which are the personal data relating to a number of individuals.

---

[14] Section I.

In addition to the IPA 2016, the RIPA 2000 contains coercive powers for surveillance (Part 2) such as monitoring a suspect's social media account and for requesting disclosure of protected data that is obtained lawfully (Part 3).

B. Interception of Content Data

1. Statutory provision

As mentioned earlier, the IPA 2016 is the key statute prescribing the interception of communication content in transmission. Accordingly, interception is unlawful by default and it gives rise criminal (s. 3), administrative (s. 7), or civil liabilities (s. 8). The interception is lawful if the person has the lawful authority to carry out that interception. The IPA 2016 contains several circumstances that render an interception lawful. These circumstances include interception carried out in relation to the consent of the sender or recipient (s. 44); by the telecommunications service provider for purposes related to the operation of the service or its enforcement (s. 45); by businesses or public authorities for monitoring or record-keeping purposes (s. 46); in certain places such as prisons, psychiatric hospitals, or immigration detention facilities (s. 47); in accordance with an international agreement (s. 52); in accordance with an interception warrant (targeted or bulk), or where it is carried out in relation to a mutual assistance warrant (s. 6).

The main interception regimes that the IPA 2016 provides are: targeted interception and bulk interception. Part 2, Chapter 1 of the IPA 2016 provides the rules for the authorisation of the latter and Part 6, Chapter 1 of the same Act governs the authorisation of the former. The targeted interception regime has three subregimes: targeted examination warrant, mutual agreement warrants, and targeted thematic warrants. Each interception regime is discussed further below. Also, the exercise of any statutory powers or the compliance with a court order to obtain communication stored in or by a telecommunication system or to take possession of any document or other property is a permissible interception within the meaning of the IPA 2016 (s. 6(1)(c)(ii)–(iii)).

2. Scope of application

a) Object of interception

According to the IPA 2016, 'interception' means 'a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if— (a) the person does a relevant act in relation to the system, and (b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication' (s. 4(1)). For the purpose of this definition, 'relevant act' in

relation to a telecommunication system means (i) modifying, or interfering with, the system or its operation; (ii) monitoring transmissions made by means of the system; or (iii) monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system' (s. 4(2)). The IPA 2016 describes the act of modifying telecommunication systems as attaching any apparatus to, modifying, or interfering with any part of the system, or any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system (s. 4(3)). The relevant time for an interception to occur is '(a) any time while the communication is being transmitted, and (b) any time when the communication is stored in or by the system (whether before or after its transmission)' (s. 4(4)).

If one party to the communications has consented to the interception, an authorisation under the Part 2 of the RIPA 2000 (on surveillance activities) is required, rather than an interception warrant under the IPA 2016. The content of communication is made 'available' even if it is recorded and made available to a person at a later time (s. 4(5)). 'Interception' as defined under the IPA 2016 does not include communications that are broadcast for general reception (s. 5(1)).

'Communication' within the meaning of the IPA 2016 includes '(a) anything comprising speech, music, sounds, visual images or data of any description, and (b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus' (s. 261(2)). Thus, communication defined as such includes the content and other data such as that related to the transmission of communication over the telecommunication service or to the operation of that service.

An important distinction for criminal law on what communication entails is the difference between the content of communication and communications data.

The IPA 2016 considers 'content' as 'any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—

a. any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and
b. anything which is systems data is not content' (s. 261(6) IPA).

Accordingly, the subject line or body of an email message is considered the content of communication. However, the first exception mentioned above means that even if a simple fact of communication may lead to some meaning, for example, by providing a link between persons or between persons and device, that data is still communications data rather than the content of communications.[15] The second exception means that data enabling or facilitating the functioning of a system or a

[15] Bulk Communications Data Code of Practice (June 2018), para. 2.57.

device is systems data (s. 263(4)) and not the content of communications even if it may reveal the meaning of the communication.

The IPA defines the term 'communications data' through overlapping sub-categories including 'systems data,' 'relevant communications data' (which may include 'events data' and 'entity data'), 'internet connection records,' 'secondary data,' and 'equipment data' (which may include 'identifying data' or 'related systems data'). The crucial point here, however, is the division between entity data and events data. This division is of particular importance because as will be discussed, the IPA 2016 requires different authorisation levels for accessing these different types of data.[16]

Accordingly, 'communications data' means entity data or events data—

a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and—
   (i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,
   (ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or
   (iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,
b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or
c) which—
   (i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,
   (ii) is about the architecture of a telecommunication system, and
   (iii) is not about a specific person,

but does not include any content of a communication or anything which, in the absence of subsection (6)(b), would be content of a communication (s. 261(5) IPA).

'Entity data' means any data which—

a) is about—
   (i) an entity,
   (ii) an association between a telecommunications service and an entity, or
   (iii) an association between any part of a telecommunication system and an entity,

---

[16] Section III.C.

b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and

c) is not events data (s. 261(3) IPA).

The above definition covers data identifiers associated with a communication such as phone numbers or IP addresses allocated to an individual or to routers; information about a person using the service such as email address, information about the devices, and information on the services to which users subscribe such as mobile phone applications installed on mobile phones.

'Events data' means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time (s. 261(4)). This definition covers the fact that someone has sent or received messages, the location where a person has made a phone call or has sent an email, Wi-Fi hotspots through which someone has connected to the internet, or the IP address of the intended receiver.

Another important definition is the 'internet connection record' (ICR) to which certain access limitation applies under the IPA 2016. Accordingly, ICR means communications data which—

a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person) (s. 63(7)).

This definition is designed to identify the specific services or applications that a user has connected to (e.g., WhatsApp) when accessing the internet through their internet access service (e.g., broadband internet connection).

b) Temporal limits of telecommunication

Prior to the adoption of the IPA 2014, the question as to which regime the interception of communications stored in a system falls into (i.e., interception regime or data acquisition regime) was answered by way of interpreting what is considered to be 'in the course of transmission' for an interception to take place. In this regard, in *Edmondson*, the UK Court of Appeal held that if the receiver of the message was totally dependent on the service provider for having access to it, then access to that stored data would fall within the remit of the interception regime as the communication would still be considered in the course of transmission.[17] Along the same lines, the IPA 2016 covers the interception of communication stored in the service

[17] *Edmondson and others v R* [2013] EWCA Crim 1026.

provider's server for further access by the receiver. As mentioned earlier, interception means that the content of communication must be made available at a 'relevant time.' That time is either during the course of the transmission of the communication or at any time when it is stored in or by the provider (s. 4(4)). This means that as long as the communication resides in the provider's server, it can be subject to interception. There is no distinction between read/unread or draft/sent emails. As long as such communication is 'in the course of transmission' at a 'relevant time,' the interception regime of the IPA 216 applies to it.

3. Special protection of confidential communication content

a) Privileged communication

The IPA 2016 introduces specific protections for communication in relation to a Member of Parliament (as defined in the relevant section), to items subject to legal privilege, to confidential journalistic material, and to sources of journalistic information (ss. 22–29).

If the information is privileged (i.e., communications between a lawyer and their client), its interception may take place if certain conditions are satisfied. If the purpose of the warrant is to obtain communications of a person who is a Member of Parliament, a Member of the European Parliament representing the UK, or a member of one of the devolved legislatures included in the relevant section, the issuing authority (the Secretary of State or the Scottish Ministers in relation to a Scottish application) has to seek the approval of the Prime Minister before issuing the warrant (s. 26(2)). As regards the interception of items subject to legal privilege, the issuing authority must consider the public interest in the confidentiality of items subject to legal privilege (s. 27(3)). There must be exceptional and compelling circumstances that make the interception necessary (s. 27(4)(a)). A warrant for items subject to legal privilege may not be issued if it is considered necessary only for the purpose of protecting the interests of economic wellbeing of the UK (in circumstances relevant to the interests of national security) (s. 27(5)). There must be arrangements in relation to handling, retention, use, and destruction of privileged items (s. 27(4)(b)). The exceptional and compelling circumstances exist if (i) the public interest in obtaining the information outweighs the public interest in the confidentiality of privileged material; and (ii) there are no other means by which the information may be reasonably obtained (s. 27(6)(a)–(b)). If the warrant is issued for the purpose of preventing and detecting serious crime or in relation to a mutual legal assistance warrant, obtaining the information must be necessary for the purpose of preventing death or significant injury (s. 27(6)(c)). Finally, the legally privileged material must be destroyed unless the IPC considers otherwise. The Commissioner can decide on the further retention of the item if it considers that the public interest in retaining the material outweighs its confidentiality, and this reten-

tion is necessary in the interests of national security or for preventing death or significant serious injury (s. 55(5)).

In relation to the interception of confidential journalistic material and sources of journalistic material, the issuing authority must consider the existence of arrangements specific to handling, retention, use and destruction of such material (ss. 28(3) and 29(3)).

b) Responsibility for ensuring protection

The IPA 2016 designates the intercepting authority as the primary body that decides on the interception of privileged material, but it also provides further conditions for that interception to be conducted. As regards warrants targeting communications of a person who is a Member of Parliament, a Member of the European Parliament representing the UK, or a member of one of the devolved legislatures, the intercepting authority applying for that warrant must make the purpose clear in their application (s. 26(1)(b)). As mentioned earlier, the Secretary of State must have the Prime Minister's approval before issuing the warrant. However, there are no additional safeguards specific to the use of the captured information.

If the purpose or one of the purposes of the interception is to obtain items subject to legal privilege, the application must make that clear (s. 27(2)). Also, if the intercepting authority believes it is likely that they will obtain items subject to legal privilege, this must be made clear in the warrant application, including an assessment of the likelihood of obtaining such items (ss. 27(7)–(8)). The Secretary of State will authorise an application if they are satisfied that there are specific arrangements on how such items are handled, retained, used, and destroyed (s. 27(9)). There are additional safeguards for the use of captured legally privileged material. Once the holder of the warrant informs the IPC of the retention of the privileged material, the Commissioner has the power to order the destruction of that item or impose specific conditions on its further use (s. 55(3)). Still, the Commissioner can direct the further retention of the respective item if they believe that the public interest in retaining the items outweighs the public interest in the confidentiality of items subject to privilege, and that retaining the item is necessary in the interests of national security or for preventing death or significant injury (s. 55(5)(a)–(b)). If that is the case, the Commissioner can still impose specific conditions as to the use of the privileged material to the extent that is necessary to protect the public interest in the confidentiality of the material (s. 55(4)).

If one of the purposes of the interception is to obtain items of confidential journalistic material, or to require the interception of communications that the intercepting authority believes will contain such material, the application for the issuance of a warrant must state this accordingly (s. 28(2)(a)–(b)). As with the arrangements in relation to items subject to legal privilege, there must be specific arrangements in place on how such items are handled, retained, used, and destroyed

(s. 28(3)). Finally, if the purpose of the interception is to obtain sources of journalistic information, the warrant application must make it clear and there must be specific arrangements on handling, retention, and destruction of the captured information (s. 29(2)–(3)).

4. Execution of telecommunication interception

a) Execution by the authorities with or without the help of third parties

The implementation of interception warrants (targeted or bulk) are carried out by the representatives of intercepting authorities listed in the IPA 2016 as being capable of requesting the issuance of such warrants (ss. 18(1) and 138(1)) with the assistance of the telecommunications operator. A non-UK entity may also apply for a targeted interception warrant if it is the 'competent authority' in accordance with the EU and international mutual assistance agreements (s. 18(2)). A technical capability notice may be served to the telecommunications operator, requesting to provide or maintain capability to carry out the interception within one working day or as specified in the notice (Part 1, sch. 1, the Investigatory Powers (Technical Capability) Regulation 2017). However, in certain circumstances, the law enforcement and intelligence agency may be able to carry out the interception itself.

Finally, the provisions of the IPA 2016 on interception (and also the provisions on other covert investigative measures under it) permits an interception warrant to be served to an entity outside of the UK (e.g., s. 41(4)), which could be a satellite operator.

b) Accompanying powers for the execution of interception

The IPA 2016 introduces investigative measures that may accompany the interception regime. As mentioned earlier, the service provider can be served a technical capability notice requesting them to comply with obligations that would enable the intercepting authority to give effect to a warrant (s. 253). One such obligation is to remove electronic protection applied to the communication (s. 253(5)(c)).

The IPA 2016 also provides equipment interference (targeted and in bulk) for certain public authorities. In this regard, the intelligence agencies (i.e., MI5, MI6, and GCHQ) request a targeted interception warrant from the Secretary of State to obtain information through securing access to equipment (i.e., 'hacking') for the interests of national security, purposes of preventing or detecting serious crime, or of protecting the economic wellbeing of the UK to the extent that this relates to the UK's national interests (s. 102). Defence Intelligence also has the power to request a targeted equipment warrant from the Secretary of State on the same grounds as requests made by the intelligence agencies (s. 104). Warrants requested by the intelligence agencies including the Defence Intelligence must be approved by the

Secretary of State who then seeks the approval of a Judicial Commissioner save in the existence of urgent cases. Finally, a law enforcement chief can issue targeted equipment warrants for the purpose of preventing or detecting serious crime (s. 106(1)). The chiefs of certain law enforcement authorities such as the NCA can issue targeted equipment warrants for purposes other than serious crime such as preventing death or any serious injury (s. 106(3)). However, officers of certain law enforcement authorities such as the Police for the City of London cannot decide on the issuance of a targeted equipment warrant unless there is a connection with the UK (s. 107). Decisions of law enforcement to issue warrants must be approved by the Judicial Commissioner except where there is an urgent need to issue the warrant without that approval (ss. 106(1)(d)–(3)(d)). As with targeted interception warrants, certain conditions apply to interfering with equipment to obtain information relating to a Member of Parliament, items subject to legal privilege, confidential journalistic material, or sources of journalistic information (ss. 111–114).

An intelligence agency can also request the Secretary of State to issue a bulk equipment interference warrant if the objective of the warrant is to obtain communications and other information on persons believed to be outside the UK. The Secretary of State may issue the warrant if it is necessary and proportionate for national security or for preventing and detecting serious crime or protecting the economic wellbeing of the UK to the extent that this is necessary for the protection of the national security interest (s. 178(1)–(2)). Save in exceptional urgent cases, the Secretary of State must seek the approval of the Judicial Commissioner before issuing the bulk equipment interception warrant (s. 178(1)).

Finally, the ISA 1994 and the Police Act 1997 provide for the authority to conduct 'property interference' where the purpose of the interference with the equipment is not for the purpose of acquiring communications data, equipment data, or other information.

5. Duties of telecommunication service providers to cooperate

a) Possible addressees of duties of cooperation

The obligation to comply with the interception warrants issued in accordance with the IPA 2016 is upon the 'telecommunication operator' which means 'a person who:

a) offers or provides a telecommunications service to persons in the United Kingdom, or
b) controls or provides a telecommunication system which is (wholly or partly)—
   (i) in the United Kingdom, or
   (ii) controlled from the United Kingdom' (s. 261(10)).

The first scenario covers situations where a person provides telecommunications service to persons in the UK, although infrastructure of that service or its establishment is located outside the UK. The second scenario relates to situations where

part of the telecommunications 'system' is located in the UK or controlled from the UK, even though it does not provide service to the UK public. Both provisions provide for the extraterritorial application of the IPA 2016 and they might give rise to conflict of laws.

A telecommunications service means 'any service that consists in the provision of access to and of facilities for making use of any telecommunication system, whether or not provided by the person providing the service' (s. 261(11)). A telecommunications system means 'a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy' (s. 261(13)). Read together, these definitions cover a wider area than is covered under EU law.[18] The reason for this difference is a deliberate choice to include services that are otherwise not covered under EU law such as Over-the-Top (OTT) services (i.e., Skype), web-based email, messaging applications and cloud-based services.[19]

Finally, the IPA 2016 does not make a distinction between private/public telecommunication operators. This means that it covers application and website providers so long as they provide a telecommunications service. Moreover, in theory, cafes, hotels, libraries, or airport lounges that offer public Wi-Fi can be subject to an interception warrant under the IPA 2016.

b) Duties to provide technical and organizational infrastructure

The cooperation duties of providers are defined for each investigative measure separately under the IPA 2016. Providers are required to take steps in giving effect to interception warrants (targeted or bulk) to the extent that they are reasonably practicable to take (ss. 43(3) and 149(5)). These steps involve technical and organisational considerations, rather than financial costs. For operators outside the UK, the requirements and restrictions of laws of the country in which they are based must be taken into account when considering what is reasonably practicable (s. 43(5)). As mentioned earlier, the operators may also be subject to technical capability notices that might impose obligations upon them including but not limited to having interception capabilities. The authority to issue a technical capability notice lies with the Secretary of State who can issue such a notice after consulting the telecommunications operator who may be the subject of the notice (ss. 253(1)(a)–(b) and 253(6)). That notice must be then approved by a Judicial Commissioner (s. 253(1)(c)). Once an operator is served a technical capability no-

---

[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201/37, 31 July 2002.

[19] Interception of Communications Code of Practice (March 2018), para. 2.6.

tice, it has the duty to comply with it. Otherwise, the Secretary of State can start civil proceedings to ensure compliance (s. 255(10)). If an operator is served a technical capability notice, the obligations under that notice are relevant to the consideration of what is reasonably practicable (s. 43(6)). Whilst the operators have to comply with obligations relating to the content data in one working day, they have to comply with obligations relating to the communications data within the time frame specified by or agreed with the Secretary of State. The Investigatory Powers (Technical Capability) Regulations 2018 details those obligations as:[20]

– To provide, modify, test, develop or maintain any apparatus, systems or other facilities or services necessary to provide and maintain the capability of interception or obtaining of secondary data.

– To provide and maintain the capability to ensure the interception, in their entirety, of all communications and the obtaining, in their entirety, of all secondary data authorised or required by a warrant.

– To provide and maintain the capability to ensure, where reasonably practicable, the transmission of communications and secondary data, as near to in real time as is reasonably practicable, to a hand-over point as agreed with the person to whom a warrant is addressed.

– To provide and maintain the capability to disclose, where reasonably practicable, only the communications the interception of which, or the secondary data the obtaining of which, is authorised or required by a warrant.

– To provide and maintain the capability to disclose intercepted communications and secondary data in such a way that communications and secondary data obtained from those communications can be unambiguously correlated.

– To ensure that any hand-over interface complies with any appropriate industry standard, or other requirement, specified in the technical capability notice.

– To provide and maintain the capability to disclose the content of communications or secondary data in an intelligible form where reasonably practicable; to remove electronic protection applied by or on behalf of the telecommunications operator to the communications or data where reasonably practicable, or to permit the person to whom a warrant is addressed to remove such electronic protection.

– To provide and maintain the capability to simultaneously intercept, or obtain secondary data from, communications relating to a number of the persons to whom the telecommunications operator provides the telecommunications service to which the communications relate which is equal to 1 in 10,000 of the persons in the United Kingdom to whom the telecommunications operator provides that service, or such smaller number as is specified in the notice.

– To ensure that any apparatus, systems or other facilities or services necessary to carry out the interception of communications or obtaining of secondary data are at least as reliable as any telecommunication system by means of which the communication that is intercepted, or the communication from which secondary data is obtained, is transmitted.

– To ensure that the capability to intercept communications or obtain secondary data may be audited so that it is possible to confirm that the communications that are intercepted, or from which secondary data is obtained, are those described in a warrant, and the integrity of the communications and data is assured so far as reasonably practicable.

---

[20] Interception of Communications Code of Practice (March 2018), Part 1.

– To ensure that the obligations imposed upon it are operated in a manner that prevents unauthorised persons becoming aware of interception.
– To notify the Secretary of State of changes to the existing telecommunications services and new developments.

c) Security requirements for data transfers by communication service providers

The Regulation made under the IPA 2016 sets forth the obligations that the technical capability notices can impose in relation to targeted and bulk interception warrants.[21] Those obligations include maintaining apparatus to conduct interception, making the transmission of communications available to a hand-over-point as near to in real time as possible, conduct interception of communication relating to up to 10,000 people in the UK simultaneously, and decrypt the communication. As for the obligation to decrypt communications, the Secretary of State must in particular take into account the technical feasibility, and likely cost, of complying with that obligation (s. 255(4)).

According to the IPA 2016, materials obtained on behalf of an authority outside the UK in the context of a mutual legal assistance and their copies can be transferred to that authority if the Secretary of State (or the Scottish Ministers in the context of a Scottish application) ensures that there are safeguards on the retention and disclosure of materials (and copies) are in place to the extent that he or she considers appropriate, and that there are restrictions prohibiting their disclosure in the legal proceedings taking place overseas (s. 54).

6. Formal prerequisites of interception orders

a) Competent authorities

Under the IPA 2016, under normal circumstances, a so-called 'double-lock' procedure is in place for the interception regime. In this regard, the Secretary of State (or the Scottish Ministers in the context of a Scottish application) has the authority to issue interception warrants (targeted or bulk) (ss. 19 and 138) according to the conditions mentioned below. However, the Secretary of State may not issue a warrant (except in urgent cases) without the decision to issue the warrant is approved by a Judicial Commissioner (ss. 19(1)(d) and 138(1)(g)). The Judicial Commissioner must review the Secretary of State's (or the Scottish Ministers in the context of a Scottish application) conclusions on the necessity of the warrant on the relevant grounds and its proportionality (s. 23). Where a Judicial Commissioner refuses to approve the warrant, the issuing authority may ask the IPC to reconsider their application (ss. 23(5) and 140(4)). If the IPC rejects the application upon reconsideration, the interception warrant (targeted or bulk) cannot be issued.

---

[21] The Investigatory Powers (Technical Capability) Regulation 2018, sch. 1.

In urgent cases, if the Secretary of State's (or the Scottish Ministers in the context of a Scottish application) reasonably considers the issuance of the warrant urgent, they can issue the warrant without the approval of the Judicial Commissioner (s. 24(1)). An urgent case exists if there is an imminent threat to life or serious harm (e.g., kidnapping) and/or an intelligence-gathering or investigative opportunity with limited time to act.[22] The issuing authority then has to notify the Judicial Commissioner of the urgent warrant (s. 24(2)). After being notified of the urgent warrant, the Judicial Commissioner must decide within three working days to approve the issuing authority's decision (s. 24(3)).

Authorities that can request the issuance of a targeted interception warrant are the heads of MI5, MI6, and GCHQ, the NCA, the Metropolitan Police; the Police Services of Northern Ireland and Scotland; HM Revenue & Customs, and the Chief of Defence Intelligence. The competent authority of a foreign country can also apply for the issuance of a targeted warrant in accordance with an international mutual legal assistance agreement in place. Upon the application of these authorities – except the intelligence agencies – the Secretary of State may issue the warrant if three conditions are met: (i) it considers that it is necessary on the grounds for which the targeted interception can be granted; (ii) the warrant is proportionate to what is sought to be achieved by it; and (iii) there are safeguards relating to the retention and disclosure of material (s. 19(1)(a)–(c)). If the head of the three intelligence agencies requests the issuance of a targeted interception, the Secretary of State must take into account, in addition to the aforementioned necessity (i) and proportionality (ii) conditions, whether the warrant may be necessary for overseas-related communication to be selected for examination (s. 19(2)).

A targeted interception warrant can be issued if it is necessary for national security interests, the purpose of preventing or detecting serious crime, or the economic wellbeing of the UK to the extent that this is also relevant to national security (s. 20(2)). A mutual assistance warrant to target communications can be issued for the purpose of giving effect to an EU or an international mutual legal assistance agreement and if the circumstance indicates that it is necessary to give effect to that agreement for the purpose of preventing or detecting serious crime (s. 20(3)). A 'serious crime' means 'crime where (a) the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or (b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose' (s. 263(1)).

---

[22] Interception of Communications Code of Practice (March 2018), para. 5.55.

A bulk interception warrant can be issued to intercept overseas-related communications (communications sent or received by persons outside the UK as defined in s. 136(3)), to obtain secondary data related to those communications, and to select examination of intercepted content or secondary data obtained under the warrant (ss. 136(2)–(4)). Such a warrant also authorises further conduct such as interception of communications or obtaining secondary data not described in the warrant if they are necessary or unavoidable to do what is required under it (s. 136(5)). This means that an interception of the communications of a person in the UK can also be carried out even if the bulk interception warrant addresses communications of a person outside the UK as due to the interconnected nature of communications it is inevitable that some communications between persons in the UK will also be intercepted. In order to examine these UK-based communications, the Secretary of State must issue a targeted interception warrant approved by the Judicial Commissioner.

'Major modifications' (i.e., adding or varying an operational purpose) to the bulk interception warrant must be subject to approval of a Judicial Commissioner (ss. 145–147). In urgent cases, those modifications may be made by the Secretary of State (s. 147). As with the scenario of issuing targeted interception warrants in urgent cases, the Secretary of State must notify a Judicial Commissioner of the modifications (s. 147(2)). The Judicial Commissioner must then decide whether to approve those modifications within three working days (s. 147(3)). If the Judicial Commissioner refuses to approve the modifications, the warrant (if it still has effect) has effect as if the modification has not been made and anything done as a result of that modification must be stopped (s. 147(4)). The Secretary of State cannot take the Judicial Commissioner's decision to refuse the major modification to the IPC for a review (s. 147(4)). 'Minor modifications' (i.e., removing an operational purpose) may be made by the Secretary of State or a senior official acting on their behalf (s. 145(6)). If minor modifications are made by a senior official, the Secretary of State must be notified of them (s. 145(7)).

The heads of the three intelligence agencies can request a bulk interception warrant. The Secretary of State may issue the warrant where it is necessary and proportionate for national security interests, the purpose of preventing or detecting serious crime, or the economic wellbeing of the UK to the extent that this is also relevant to national security. A bulk interception warrant may relate to one or more specified purposes, but the national security interest must always be one of those purposes (s. 138(1)(b)).

b) Formal requirements for applications

An application for an interception warrant (targeted or bulk) is made in written form and includes the draft interception warrant (including the draft instrument and schedules) and application form. The content of an interception warrant (targeted or

bulk) is listed in IPA 2016 and the Interception of Communications Code of Practice. In this regard, a targeted warrant application must specify its type (targeted warrant, targeted examination warrant, or mutual assistance warrant), the grounds on which it is sought, the background to the operation or investigation, the details of the persons, organization, or set of premises, the details of the communications to be intercepted or the secondary data to be obtained, the details of the telecommunications operator and an assessment on the feasibility of interception, how the interception is expected to be beneficial for the investigation or the operation, the description of the conduct that will be expected to be carried out, consideration of the proportionality of the interception including whether what is sought by the warrant could be reasonably achieved by other less intrusive means, where the purpose of the interception is to obtain communications of relevant legislature (Members of Parliament, Members of Scottish Parliament, etc.[23]) or privileged material[24] a statement indicating that purpose and in the case of the latter the details of the arrangements for handling, retention, use, and destruction of such material, where the application is urgent a statement justifying this circumstance, and an assurance on the safeguards relating to the retention and disclosure of material.

An application for a bulk interception warrant must specify the background to the application, the description of the communications to be intercepted, the details of telecommunications operator(s) who may be required to assist, an assessment on the feasibility of the operation, the description of the conduct to be authorised (which has to be limited to overseas-related information), the operational purpose for which the content or the secondary data may be selected for examination, consideration whether the intercepted content or the secondary data may be made available to other intelligence agencies or an international partner to the extent that it is necessary and proportionate to do so, an explanation on why the conduct is necessary for one or more statutory purposes which must include the explanation on why it is necessary for the national security interest, consideration of the proportionality of the interception including whether what is sought by the warrant could be reasonably achieved by other less intrusive means, an assurance on limiting the selection of obtained material for examination to the extent that is necessary for the statutory grounds specified in the warrant and on the existence of safeguards relating to the examination of that material, and an assurance on the safeguards relating to the retention and disclosure of material.

c) Formal requirements for orders

An interception warrant (targeted or bulk) consists of an application form and the draft warrant (including the draft instrument and schedules). Although the submis-

---

[23] IPA 2016, s. 26.

[24] Section III.B.3.

sion of investigative files is not required, as mentioned earlier, for a targeted interception warrant the details of the investigation or operation for which the interception is sought must be included in the draft warrant. Applications for a bulk interception warrant may specify the background.

7. Substantive prerequisites of interception orders

a) Degree of suspicion

Although the IPA 2016 does not explicitly mention a degree of suspicion necessary for interception, an interception warrant would not be granted unless there is evidence that it concerns a serious crime, which may have occurred in the past or will occur in the future.

b) Predicate offences

As mentioned earlier, the grounds for which an interception warrant (targeted or bulk) can be issued are: national security interests, the purpose of preventing or detecting serious crime, or the economic wellbeing of the UK to the extent that this is also relevant to national security (ss. 20(2) and 138(1)(b)–(2)). Therefore, in terms of crimes that justify an interception warrant, the IPA 2016 limits it to 'serious crime'; that is 'crime where (a) the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or (b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose' (s. 263(1)). According to this definition, the qualifications for serious crime (thus one of the purposes for granting interception) are: the minimum punishment threshold, or 'the use of violence' for substantial financial gain, or acting for a common purpose. As noted above, the UK Government changed the definition of serious crime and lowered the minimum threshold from 3 years or more to 12 months.[25]

c) Persons and connections under surveillance

A targeted interception warrant may relate to a particular person, or organisation, or a single set of premises (s. 17(1)). For the purpose of the IPA 2016, a person can be an individual as well as a legal person because the term includes a body of persons corporate or unincorporated.[26] Moreover, an 'organisation' includes entities

---

[25] Section III.C.1.

[26] The Interpretation Act 1978, sch. 1.

that are not legal persons such as a particular company.[27] A 'set of premises' may include land, an aircraft, or a vehicle.[28]

A targeted interception warrant can be authorised not only in relation to suspects, but also those who are not suspects but whose communications might be beneficial for the investigation. The IPA 2016 allows for interception warrants that relate to certain subject matters. This kind of warrant is called a 'targeted thematic warrant' and it can cover '(a) a group of persons who share a common purpose or who carry on, or may carry on, a particular activity; (b) more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation; (c) testing or training activities' (s. 17(2)). Examples of a targeted thematic warrant are the interception of communications of three people in relation to a single investigation of money laundering or the interception of online material in order to identify those who search for child pornography material online.

The IPA 2016 allows for the interception of communications targeting particular communication content with its bulk interception regime. As mentioned earlier,[29] a bulk interception warrant can only be requested by the three intelligence agencies and must relate to the interception of overseas-related communications and/or obtaining of secondary data from such communications. Bulk interception works through capturing overseas-related communications from the communications links or signals that the intercepting authority has chosen to intercept. These captured communications are then filtered to select those communications with intelligence value. Those selected communications are retained to analyse those with the greatest intelligence value. These latter communications can then be examined for the operational purposes indicated in the bulk examination warrant.[30] If the intelligence agency wants to examine the content of communications of a person believed to be in the British Islands that was intercepted under a bulk interception warrant, it must separately apply for a targeted examination warrant under which the selection of the intercepted content for examination can be carried out (s. 15(3)).

d) Principle of subsidiarity

As mentioned above, intercept evidence is inadmissible before the UK courts. Nevertheless, the authority requesting for interception (targeted or bulk) must indicate in its application why other less intrusive means of investigation cannot achieve what it sought to achieve with the interception. Also, when deciding whether the interception is necessary and proportionate, the Secretary of State must

---

27 Interception of Communications Code of Practice (March 2018), para. 5.8.

28 Ibid., para. 5.9.

29 Section III.B.

30 Interception of Communications Code of Practice (March 2018), para. 6.6.

consider whether what is sought to be achieved could reasonably be achieved by other less intrusive means (s. 2(2)(a)).

e) Proportionality of interception in individual cases

The IPA 2016 states that where a targeted interception is considered necessary only to gather evidence for use in any legal proceedings, that interception may not be considered necessary for the statutory grounds upon which an application for such interception can be made (s. 20(5)). Also, bulk interception can only be carried out for intelligence purposes and not in relation to criminal proceedings.

The Secretary of State must consider whether each application for an interception warrant (targeted or bulk) is proportionate as well as necessary for achieving the statutory grounds for which each type of interception can be sought. In considering whether a warrant is necessary and proportionate, the Secretary of State must take into account whether there are other less intrusive means that can reasonably achieve what is sought by the warrant (s. 2(2)(a)).

f) Consent by a communication participant to the measure

Where one of the parties to the communication has consented to the interception, an interception warrant is not required (s. 44(1)). However, this conduct is considered a form of surveillance and requires authorisation under Part 2 of Regulation of Investigatory Powers Act 2000. This authorisation is different to the authorisation regime for interception under the IPA 2016.

8. Validity of an interception order

a) Maximum length of an interception order

Under normal circumstances, interception warrants (targeted or bulk) are valid for an initial period of 6 months. A targeted interception warrant issued under the urgency procedure is valid for 5 working days following the issuance of the warrant unless renewed by the Secretary of State.

b) Prolongation of authorisation

Upon renewal, an interception warrant (targeted or bulk) is valid for another 6 months starting from the day after it would have otherwise expired (ss. 32(2)(b)(ii) and 143(2)). A warrant may not be renewed more than 30 days in advance of the warrant ceasing to have effect (ss. 33(5)(b) and 144(3)).

In order to be renewed, a targeted interception warrant must remain necessary and proportionate, applying the same tests and procedure as for issuing a warrant.

The additional safeguards for Members of Parliament and for other privileged materials[31] apply as if issuing a warrant. The renewal decision must be taken by the Secretary of State. The decision to renew a bulk interception warrant must be approved by the Judicial Commissioner (s. 33(7)).

As regards a bulk interception warrant, the Secretary of State must believe that the warrant continues to be necessary and proportionate in relation to one of the relevant statutory grounds, and that the operational purposes continue to be necessary (s. 144(2)). The decision to renew the bulk interception warrant must be approved by the Judicial Commissioner (s. 144(5)).

c) Revocation of authorisation

The Secretary of State (or the Scottish Minister where relevant) or a senior official acting on behalf of the Secretary of State may cancel a targeted warrant issued under Part 2, Chapter 1 of the IPA 2016 at any time if he or she decides that the warrant is no longer necessary or proportionate or the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved (s. 39). A bulk interception warrant may also be cancelled by the Secretary of State or a senior officer acting on behalf of the Secretary of State where he or she is satisfied that the warrant is no longer necessary in the interests of national security, the authorised conduct is no longer proportionate to achieve the aim it sought, or the examination of intercepted content or secondary data obtained under the warrant is no longer necessary for any specified operational purposes (s. 148).

If the conditions to cancel an interception warrant (targeted or bulk) are met, the Secretary of State must cancel the warrant (ss. 39(2) and 148(2)).

9. Duties to record, report, and destroy

a) Duty to record and report

The IPA 2016 designates the IPC as the public authority for overseeing its implementation. It also maintains the ex-post facto oversight mechanism, the Investigatory Powers Tribunal (IPT), to which individuals can bring a claim in relation to the implementation of the IPA 2016. According to the Interception of Communications Code of Practice, all authorities involved in the interception regime must keep records at least three years, or up to five years if possible and make those records available to the IPC and the IPT.[32] Additionally, each intercepting authority must keep information in relation to the targeted interception warrants they applied for such as the number of warrants that have been applied for or refused by the Secre-

---

[31] Section III.B.3.

[32] Interception of Communications Code of Practice (March 2018), para. 10.01.

tary of State, and the number of warrants issued in urgent cases, renewed, or cancelled for every calendar year to assist the IPC in carrying out their statutory obligations. Along the same line, the intelligence agencies must keep information in relation to the bulk interception warrants they sought such as the number of applications, refusals, and renewals in order to assist the IPC. They also have to record certain information such as the statutory grounds for which the bulk interception warrants have been sought, operational purposes specified in the warrants, and details of modifications that have been made.

Finally, the intercepting authority or telecommunications operator must report to the IPC any error that they are aware occurred while that author was complying with the requirements of the IPA 216 (s. 235(6). The Interception of Communications Code of Practice outlines the circumstances for which an error within the meaning of the IPA 2016 may occur. Those circumstances are:[33]

– the interception of communication without lawful authority;
– where obtaining of secondary data occurred not in accordance with a warrant (targeted or bulk);
– failure to adhere to the safeguards relating to the retention and disclosure of the material, and its transfer outside the UK.

Examples of error under these circumstances are:[34] human error; warranted interception taking place at a communication address but not relating to the intended person or premises; failure to cease the interception where the warrant is cancelled; a breach of safeguard due to software or hardware errors; where the selection for examination of bulk content or secondary data is done for a purpose that is not specified in the warrant; the retention of material obtained under a warrant longer than that is necessary for the warrant's purpose; the unauthorised selection for examination of content relating to a person in the British Islands; or the unauthorised selection of material for examination is carried out to obtain items subject to legal privilege.

b) Duty to destroy

The intercepting authorities must destroy materials obtained through interception warrants (targeted or bulk) and their copies as soon as there are no longer any relevant grounds for retaining them (ss. 53(5) and 130(5)). The IPA 2016 defines 'destroy' as to 'delete the data in such a way as to make access to the data impossible (and related expressions are to be read accordingly)' (s. 263(1)), but it does not provide a procedure for the destruction of records.

---

[33] Interception of Communications Code of Practice (March 2018), para. 10.14.

[34] Ibid., para. 10.15.

10. Notification duties and remedies

a) Duty to notify persons affected by the measure

The investigative authorities do not have a duty to inform intercepted persons about an interception. Any unauthorised disclosure about an interception such as by the telecommunications operator or the intercepting authority is a criminal offence under the IPA 2016 that may give rise to a fine or maximum 12 months of imprisonment (s. 59).

b) Remedies

As mentioned earlier, if a person becomes aware of the interception, they can bring legal proceedings (s. 65(2)(a) or (d) RIPA 2000) or can make a complaint or reference (s. 65(2)(b)–(c) RIPA 2000) to the IPT. They can also appeal to the decisions of the IPT on a point of law or where there is a compelling reason for an appeal (s. 242 IPA 2016).

The IPT has no duty to hold oral hearings, but it may do so for certain circumstances such as requiring the person whose conduct is the subject of the complaint to give evidence (Rule 9(2)–(4) of the Investigatory Powers Rule Tribunals 2000). Those oral hearings and the IPT's proceedings shall be conducted in private (Rule 9(6) of the Investigatory Powers Rule Tribunals 2000). Nevertheless, the IPT can use its discretion to hold oral proceedings in public subject to its duty to prevent disclosure of sensitive information.[35] The IPT upholds very few complaints. For example, from 2012 to 2016, 15 out of 1,002 cases were held in favour of the complaint.[36]

c) Criminal consequences of unlawful interception measures

Illegal interceptions by the intercepting authorities do not give rise to particular sanctions. Nevertheless, the IPA 2016 obliges those authorities and telecommunications operators to the extent of their knowledge to inform the IPC of any error in relation to giving effect to a targeted or bulk interception warrant (s. 231). According to the 2016 bi-annual report of the IOCCO, which was superseded by the IPC with the introduction of the IPA 2016, the total number of interception errors during 2016 was 108.

There are two ex-post mechanisms to monitor public authorities' interception powers. The first mechanism is, as mentioned earlier, the IPC established under the IPA 2016 (ss. 227 et al.). The IPC assumes oversight of the role of public authorities' investigatory powers including those under the IPA 2016 previously held by

---

[35] Appl. No. IPT/01/62 and IPT/01/77 (23 January 2003).

[36] Investigatory Powers Tribunal, Statistical Report (2016), available at https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

the IOCCO, the OSC, and the ISC. The IPC is appointed by the Prime Minister and must hold or have held a high judicial office (s. 227(1)(a)–(b)).

The second mechanism is the IPT. As mentioned earlier, persons can bring legal proceedings, and make complaints or references to the IPT when they become aware of the interception. With the introduction of the IPA, they can also appeal against the decisions of the IPT. The independent nature of the IPT was tested before the ECtHR in *Kennedy* where the Court held that the IPT met the requirements of the ECHR.[37]

11. Confidentiality requirements

Internet providers are obliged to not to disclose information about any interception with which they have assisted (s. 57). Infringements of this obligation would be a criminal offence giving rise to a fine or maximum 12 months of imprisonment (s. 57). A corporate officer of the operator could be held personally liable for unauthorised disclosure (s. 266).

According to the Interception of Communications Code of Practice, all interception systems must comply with any security policies and standards in place in relation to the interception of communications, including those policies set forth by the Secretary of State or by the NTAC. These policies and standards cannot be made public because their disclosure may create security risks.[38] Technical capability notices served in accordance with the IPA 2016 may also oblige telecommunications operators to develop data security policies such as access controls, or the security and integrity of interception capabilities.[39]

C. Collection and Use of Traffic Data and Subscriber Data

1. Collection of traffic data and subscriber data

Part 4 of the IPA 2016 provides for the retention of 'communications data' by a telecommunications operator whereas its Part 3 relates to the statutory powers of certain public authorities to acquire such data from the operator. As mentioned above, 'communications data' comprises the 'events data' that relates to the attributes of the communications and the 'entity data' that relates to what is generally known as subscriber data. There are also certain restrictions on access to the internet connection records, which is the information held by the telecommunications operator about the service via which the customer is connected to the internet (s. 62(7)).

---

[37] *Kennedy v United Kingdom* [2010] ECHR 682

[38] Interception of Communications Code of Practice (March 2018), paras. 8.78–8.79.

[39] Ibid., paras. 8.80–8.82.

a) Collection of traffic data

The IPA 2016 is the key legislation for the powers of public authorities to access traffic data (or in the terms of the IPA 2016, 'events data'). Designated senior officers of certain public authorities may confer on officers in each authority the power to request access to traffic data from the telecommunications operator (s. 61(2)). The means access to traffic data (e.g., through an online procedure) depends on the process agreed with the service provider. A request for data acquisition can be made if it is necessary and proportionate to achieve the following ends (s. 61(7)):

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- in the interests of the economic wellbeing of the United Kingdom so far as those interests are also relevant to the interests of national security;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- to assist investigations into alleged miscarriages of justice;
- where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—
  - to assist in identifying P, or
  - to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition, or
- for the purpose of exercising functions relating to—
  - the regulation of financial services and markets, or
  - financial stability.

Those authorities are:[40]

- Police Forces;
- Regional Police Forces;
- Ambulance services;
- Her Majesty's Revenue and Customs;
- Competition and Markets Authority;
- Criminal Cases Review Commission;
- Department for the Economy in Northern Ireland;

[40] IPA 2016, sch. 4.

- Department of Health;
- Anti-Fraud Unit;
- Department for Transport;
- The Maritime and Coastguard Agency;
- Department for Work and Pensions;
- Financial Conduct Authority;
- Fire and rescue authorities;
- Food Standard Agency;
- Gambling Commission;
- Gangmasters and Labour Abuse Authority;
- Health and Safety Executive;
- Independent Police Complaints Commission;
- Information Commissioner's Office;
- Ministry of Justice;
- National Health Service Business Service Authority;
- Office of Communications;
- Serious Fraud Office;
- Home Office.

Schedule 4 of the IPA 2016 details the exclusive purposes for which the designated officer of each mentioned authority has the power to acquire the traffic data. For example, the Department of Health can access the data for three purposes; detecting crime and public disorder, in the interest of public safety, or for protecting public health. Finally, local authorities can get access to the data if it is necessary for the purposes of a specific investigation or authorisation, or for detecting and preventing crime or public disorder (s. 73(3)). However, they cannot access internet connection records (s. 62(1)).

A request for communications data may involve obtaining the data by the authorised officers themselves from the telecommunications operator (s. 61(4)(a)), or requiring the operator to disclose the data that is already in its possession or that it is capable of obtaining (s. 61(4)(c)).

In order to get access to the retained data, the authorised officer must contact the Single Point of Contact (SPoC), which is an accredited individual or group of individuals trained to facilitate the lawful acquisition of communications data. After consideration, the SPoC advises the officer, who must consider the most appropriate method for obtaining the data concerned, on the cost and the resources for the requested access, any unintended consequences, and any issues as to the unlawfulness of the access authorisation (s. 76(5)). Any authorisation for access to retained data for identifying or confirming journalistic sources must be approved by a Judicial Commissioner (s. 77). The telecommunications operators have the statutory duty to comply with the data acquisition notices to the extent that it is reasonably practicable for them to do so (s. 66(1)–(3)). Otherwise the Secretary of State may start civil proceedings to enforce those notices through injunction or specific per-

formance (s. 66(5)). However, in practice, the Secretary of State has not resorted to the judicial remedy. As mentioned earlier, the IPA 2016 has extraterritorial scope that covers the circumstances in which the powers enshrined under it may be imposed upon non-UK based operators.[41] This means that data acquisition notices can be served to providers of services located outside the UK, requesting data about a UK subscriber. Inevitably, this may give rise to a conflict of laws between the UK and the laws of the country in which that provider is based.

However, the Data Retention and Acquisition Regulations 2018 changed the acquisition of communication data regime discussed above. For example, the Information Commissioner will authorise the relevant public authority to obtain communications data if he or she considers that it is necessary and proportionate to what is sought to be achieved (s. 5). Also, the purposes for which communications data may be accessed changes from the purpose of preventing and detecting crime and public order to 'applicable crime purpose,' which is formulated as '(a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime; (b) in any other case, the purpose of preventing or detecting crime or of preventing disorder' (Regulation 5). As mentioned earlier, the threshold of imprisonment to qualify 'serious crime' within the meaning of the IPA 2016 changes from 3 years to a 12 month custodial sentence.

b) Collection of subscriber data

Subscriber information would fall within the meaning of 'entity data,' a subcategory of communications data, under the IPA 2016.[42] The requirements for accessing entity data are the same as for events data except that the IPA 2016 allows low-level staff to request internally the authorisation to access the entity data (sch. 4). This difference persists in the draft Data Retention and Acquisition Regulations 2018, access to events data may be authorised for the purpose of the prevention or detection of serious crime, but a request solely for entity data may be made for the purpose of the prevention or detection of crime or of preventing disorder.

A dynamic IP-address identifies the routing information through which an apparatus is used, and thus falls within the meaning of 'events data' as defined under the IPA 2016. For this reason, the procedure explained above in relation to traffic data is applicable to its acquisition by public authorities.

As mentioned earlier, subscriber information relates to 'entity data' under the IPA 2016. This means that they would fall within the data retention regime provided under the same Act. Internet providers would also be considered to be a 'telecommunication operator' to the extent that they provide a 'telecommunications

---

41 Section I.A.3.

42 Section III.B.2.a.

service' within the meaning of the IPA 2016. Thus, internet providers may be served a notice by the Secretary of State, obliging them to retain certain communications data for a maximum period of 12 months (ss. 87(1)–(3)). The Secretary of State may give such notice if they consider that the retention is necessary and proportionate for the same purposes as in the acquisition of the traffic data mentioned earlier (ss. 87(1)(a)).

Just like the double-lock procedure for the issuance of an interception warrant, a data retention notice from the Secretary of State must be approved by a Judicial Commissioner (s. 87(1)(c)). Upon receiving the notice, the telecommunications operator must secure the integrity of the data and put appropriate technical and organizational measures in place to protect the data against accidental or unlawful destruction, loss or alteration, retention, processing, access, and disclosure (s. 92).

The draft Data Retention and Acquisition Regulations 2018 amends the data retention regime under the IPA 2016, just as it amends the acquisition regime. For example, it restricts the purposes for which the Secretary of State may give a notice to a telecommunications or postal operator requiring the retention of communications data. A notice may be given where it is necessary and proportionate to retain data in the interests of national security or of the economic wellbeing of the UK so far as relevant to national security, in the interests of public safety, for the purpose of preventing death or injury or to assist investigations into alleged miscarriages of justice. A notice in relation to events data may be given for the purpose of the prevention or detection of serious crime, or in relation to entity data for the purpose of the prevention or detection of crime or of preventing disorder.

c) Data retention

Traffic data would fall within the meaning of 'events data' defined under the IPA 2016 and the Secretary of State may oblige its retention by the telecommunications provider in accordance with the same procedure required for the retention of entity data and for a maximum period of 12 months. Thus, the fact that someone received an email, date and time of connection, connection points through which the user makes use of the telecommunication service such as Wi-Fi hotspots, or the IP addresses of an intended receiver of an email may be required to be retained under a retention notice. Insofar as the data retention regime is concerned, there is no difference between the procedure and safeguards applicable to the retention of the events data and the entity data as the sub-categories of communications data. The difference arises in relation to the procedure to access this retained data.[43]

---

[43] Section III.C.

2. Identification of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

There is no specific provision on the use of IMSI catchers under the UK law. However, the UK Government has neither permitted nor prohibited the use of IMSI catchers. Property and wireless telegraphy interference powers under Part 3 of the Police Act 1997 and s. 5 Intelligence Service Act 1994 may cover their use.[44] In this context, under the former regime, the services police, National Crime Agency (NCA), HM Revenue and Customs (HMRC), Competition and Markets Authority (CMA), Independent Office for Police Conduct (IOPC), Police Investigations and Review Commissioner, or Home Office (for departments exercising functions relating to immigration matters, and officers designated as customs officials), or persons acting on their behalf may apply to the authorised officer for an authorisation for property interference (s. 93(3)) as long as the act does not otherwise constitute an offence under the Computer Misuse Act 1990. Under the latter regime, the Secretary of State may authorise property interference on the application of the Security Service, GCHQ, and the Intelligence Service. The use of IMSI catchers may also fall within equipment interference under the IPA 2016, details of which are discussed below, where the conduct would otherwise constitute an offence under the Computer Misuse Act 1990 and there is a British Islands connection.[45] Finally, they also constitute interception under the IPA 2016.

D. Access to (Temporarily) Stored Communication Data

1. Online searches with the help of remote forensic software

The IPA 2016 provides rules to authorise equipment interference by the intelligence agencies (MI6, MI5, GCHQ) defence intelligence and law enforcement agencies to obtain communication, information, or equipment data, that is, data that enables or identifies the functioning of a system (i.e., 'systems data' as defined under s. 263(4) IPA 2016) and that may be used to identify any person, apparatus, system, event, or the location of any person, event, or thing (i.e., 'identifying data' as defined under s. 263(2)–(3) IPA 2016)) (s. 99(2)). It also confers powers upon the intelligence agencies to conduct equipment interference without a certain target for the purpose of obtaining overseas-related communication, information, or equipment data. In this context, equipment interference covers the power of the

---

[44] HC Deb 7 July 2015 c 5369, available at https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2015-07-02/5369

[45] What the UK's Proposed Surveillance Law Means for Police Hacking, Joseph Cox (motherboard.vice.com, 26 February 2016), https://motherboard.vice.com/en_us/article/yp3vxb/what-the-uks-proposed-surveillance-law-means-for-police-hacking

authorities to interfere with equipment remotely such as through installing software or physically such as through accessing USB ports.

The former powers are referred to as targeted equipment interference. The purposes for and the procedure through which a public authority may apply for the issuance of a targeted equipment interference warrant differs between intelligence and law enforcement agencies. The head of an intelligence agency may apply to the Secretary of State for a warrant if it is necessary in the interests of national security, for the purpose of preventing and detecting serious crime, or in the interests of the economic wellbeing of the UK so long as this is relevant for national security (s. 102(5)). The Chief of Defence Intelligence may apply for a warrant only in relation to the interests of national security (s. 104). Upon an application by either authority, the Secretary of State may issue a warrant if they consider that it is necessary and proportionate to achieve the aim, there are safeguards in relation to the retention and disclosure of material in place, and with the approval of a Judicial Commissioner except where the Secretary of State considers there is an urgent need to issue the warrant (ss. 102(1)–104(1)).

In terms of the targeted equipment interference powers of law enforcement agencies, a law enforcement chief may issue a warrant authorising such interference where they consider that the warrant is necessary for the purpose of preventing or detecting serious crime and that the conduct authorised is proportionate (ss. 106(1)(a)–(b)) and where they are satisfied that safeguards in relation to the retention and disclosure of material are in place (s. 106(1)(c)). A law enforcement chief must seek the approval of a Judicial Commissioner for the warrant if they consider there is an urgent need to issue the warrant (s. 106(1)(d)). Certain law enforcement officers as defined under sch. 6 IPA 2016 may issue a warrant for purposes other than serious crime, that is, for the purpose of preventing death or any injury or damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health (s. 106(3)(a)). Finally, certain law enforcement officers such as the Commissioner of the Metropolitan Police Force or the Chief Constable of the Ministry of Defence Police may not issue a targeted equipment interference warrant if there is no connection with the British Islands (s. 107).

In relation to the application made by the intelligence agencies, the Secretary of State must seek the approval of the Prime Minister if the targeted equipment warrant concerns obtaining communications of a person who is a Member of Parliament, etc. (s. 111(1)–(3). For the targeted equipment interference carried out by the law enforcement, the law enforcement officer must seek both the Secretary of State and the Prime Minister's approval for warrants issued for the purpose of obtaining communications of the mentioned persons (s. 111(4)–(7)). There are certain safeguards which apply to targeted equipment interference for items subject to legal privilege, such as the duty of the issuing authority to consider the public interest in the confidentiality of those items (s. 112). Along the same lines, the IPA 2016 provides certain safeguards which apply to targeted equipment interference for confi-

dential journalistic material and sources of journalistic material, such as those in relation to the handling, retention, use, and destruction of that material (ss. 113–114).

A targeted equipment interference warrant (on the application of both intelligence and law enforcement agencies) lasts six months unless renewed in accordance with the required renewal procedure (ss. 116–117). It is the statutory duty of the telecommunications operator, to the extent that it is reasonably practicable, to comply with a targeted equipment interference warrant and this duty is enforceable through civil proceedings (s. 128). Any authorised disclosure of the existence or the details of targeted equipment interference warrant such as by a telecommunications operator would be an offence under the IPA 2016 (ss. 132–134).

The power of the intelligence agencies to carry out equipment interference without a certain target is referred to as bulk equipment interference (Part 6 Chapter 3). There are two conditions under which that interference can be conducted. The first condition is that it must be for the purpose of obtaining overseas-related communications, overseas-related information or overseas-related equipment data. This means that a bulk equipment interference cannot be issued if the primary purpose is obtaining communications between individuals in the British Islands or the information of individuals in the British Islands. The second condition is that the warrant must authorise the obtaining of communications, equipment data and other information to which the warrant relates, and may also authorise the selection for examination of material obtained under the warrant. The intelligence agencies may apply for the issuance of a bulk equipment interference warrant to the Secretary of State, who may issue such warrant if it is necessary and proportionate for one or more statutory purposes. One of such purposes must be the interests of national security (s. 178(1)). Other statutory purposes are the prevention and detection of serious crime or the interests of the economic wellbeing of the UK so long as this purpose is relevant for the interests of national security (s. 178(2)). Except in urgent cases, the Secretary of State must seek the approval of a Judicial Commissioner before issuing the bulk warrant (s. 178(1)(f)). The duration of a bulk equipment interference is six months under normal circumstances and five working days in urgent cases, unless renewed (s. 184). As with the rules on the implementation of the targeted equipment interference warrants, telecommunications operators are under a statutory duty (to the extent that is reasonably practicable) to comply with the bulk warrant. Otherwise, the Secretary of State may start civil proceedings to enforce that warrant (s. 190(5)). There are also certain safeguards in relation to the obtaining of items subject to legal privilege, such as the existence of exceptional and compelling circumstances for the selection of such items, and of confidential journalistic material, such as the duty to inform the Investigatory Powers Commissioner as soon as reasonably practicable (ss. 194–195). The duty to not to make unauthorised disclosures applies to a bulk equipment interference warrant as it applies to a targeted warrant (s. 197).

2. Search and seizure of stored communication data

There are a number of laws that provides for the rules on the search and seizure for stored electronic communication data, such as:

– Proceeds of Crime Act 2002, s. 345;
– Police and Criminal Evidence Act (PACE) 1984, s. 9;
– Terrorism Act 2000, sch. 5.

Under the Proceeds of Crime Act 2002, a production order may be issued if there are reasonable grounds suspecting that the person is subject to money laundering investigations (s. 346(2)). This may be issued if there are reasonable grounds for believing that the person in question is in possession or control of the material requested (s. 346(3). There must also be reasonable grounds believing that the material is likely to be of substantial value for the investigation and that it is in the public interest to produce the material or have access to it taking into account its benefit for the terrorist investigation and the circumstances under which the person concerned appears to have the material in his possession or control (s. 346(4)–(5)).

According to sch. 1 PACE 1984, a constable may apply to a circuit judge to make an order that material should be produced or that access to it should be given in relation to s. 9 of the same Act. A circuit judge may make such order if he is satisfied that the following three conditions exist: (i) there are reasonable grounds for believing that an indictable offence, which means an offence triable on indictment before the Crown Court, has been committed; that there is material which consists of special procedure material; that the material is likely to be of substantial value and to be relevant evidence, (ii) other methods of obtaining material have been tried without success; or have not been tried because it appeared that they were bound to fail, and (iii) there is public interest to make that order taking into account the benefit of the requested material for the investigation and the circumstances under which the person in possession of the material holds it (sch. 1).

Schedule 5 of the Terrorism Act 2000 gives a constable or counter-terrorism investigator the power to apply to a circuit judge to issue a production order for the purposes of a terrorist investigation. The order may require a specified person to produce or to give access to material which he has in his possession, custody, or power within a specified period (sch. 5 para. 5). It may also require a specified person to state to the best of his knowledge the location of the material if it is not in, and will not come into his possession, custody, or power within that specified period (sch. 5 para. 5(3)). Unless specified otherwise in the order, the specified person has to comply with the order within seven days of the date of the order (sch. 5 para. 5(4)). Upon request by the relevant authority, a circuit judge may grant a production order if they are satisfied that the requested material consists of excluded material (as defined in s. 11 Police and Criminal Evidence Act 1984, which includes trade records and journalistic material) or special procedure material (as

defined in s. 14 PACE 1984, which includes journalistic material other than excluded material); that it does not include items subject to legal privilege, that it is sought for the purposes of a terrorist investigation; that there are reasonable grounds to believe that the material is likely to be of substantial value for a terrorist investigation; that there are reasonable grounds to believe that it is in the public interest that the material requested should be produced or be given access to taking into account its benefit for the terrorist investigation and the circumstances under which the person concerned has the requested material in his possession, custody, or power (sch. 5 para. 6). Unless the order states otherwise, the person has to comply with the order within 28 days of the date of the order. A person in the possession of the requested material shall produce it to a constable or give a constable access to it not later than the end of the period of seven days from the date of the order or the end of any longer period that the order may specify.

The provisions of the IPA 2016 on the search and seizure of stored communications data do not supersede or replace other powers under the UK law to obtain stored data (s. 6(1)(c)(ii)); examples of which provided above. It is arguable whether the data retention regime under the IPA 2016 provides a higher degree of legal protection for the suspect than the regime under the PACE 1984.

Access can be had to the stored data without notifying the suspect where such notification would prejudice the investigations due to the threat that the evidence might be destroyed. The service provider would be aware of the order.

3. Duties to cooperate: production and decryption orders

As mentioned earlier, the IPA 2016 provides for a regime of technical capability notices through which the telecommunications operator may be requested to remove any encryption that it applied to the service.[46] Access to the encrypted data can also be carried out in accordance with the powers conferred upon the law enforcement agencies under Part 3 of the RIPA.

A person may be subject to a notice requiring them to either provide information in an intelligible format or to disclose the 'key' to access the protected data. Under RIPA, 'protected information' means 'any electronic data which, without the key to the data— (a) cannot, or cannot readily, be accessed, or (b) cannot, or cannot readily, be put into an intelligible form' (s. 56(1)). A 'key' is 'any key, code, password, algorithm, or other data the use of which (with or without other keys): (a) allows access to the electronic data, or (b) facilitates the putting of the data into an intelligible form' (s. 56(1)).

A suspect in an investigation may be subject to that notice requiring them to disclose an encryption key. It is an offence if a person 'knowingly fails, in accordance

---

[46] Section III.B.4.b.

with the notice, to make the disclosure required …,' which carries a maximum two-year prison term (s. 53). Under the Terrorism Act 2006, this penalty was increased in 'a national security case' to five years. A five-year term has also since been inserted in respect of 'child indecency' cases.

The validity of these provisions was examined in *R v S and A*.[47] The defendants were both arrested in connection with terrorist offences. S was detained in a room where an encryption key appeared to have been partially entered into the computer. In the case of A, computer materials seized subsequent to his arrest included a computer disc that contained an encrypted area. The defendants appealed against the notices issued under s 49 of the RIPA requiring that they disclose the encryption keys on the grounds of self-incrimination. The court noted that the legality of this process had to be addressed in two stages. The first question was to determine whether the principle was engaged at all. Relying upon the ECtHR decision in *Saunders*,[48] the court noted that the right not to self-incriminate does not extend to material that can be lawfully obtained by law enforcement and has 'an existence independent of the will of the suspect'. The key, irrelevant of the form in which it exists, was held to be such an independent fact, similar in nature to a urine sample taken from a driver suspected of driving under the influence. However, in addition, it was noted that the defendant's knowledge of the key could also be an incriminating fact. The second stage for the court, if it is assumed that the principle is engaged, is to consider whether the interference with the right stemming from the issuance of the s. 49 notice is necessary and proportionate. Here the court held that the procedural safeguards and limitations on usage detailed in the RIPA were sufficient to negate any claim of unfairness under s. 78 PACE.[49]

IV. Use of Electronic Communication Data in Judicial Proceedings

1. Use of electronic communication data in the law of criminal procedure

The IPA 2016 prohibits intercepted communications being used or disclosed before the UK courts in civil and criminal proceedings, and inquiries (s. 56) unless certain exceptional circumstances exist (sch. 3). The reason for this prohibition is to exclude the operation of the intelligence and law enforcement agencies from examination.

---

47 [2008] EWCA Crim 2177.

48 [1996] 23 EHRR 313.

49 Section IV.1.

That said, the material obtained through an interception warrant would be admissible if it does not reveal anything about the activities of UK law enforcement agencies, such as if the telecommunications operator carries out an interception in order to enforce the provisions of the Communications Act 2003 in accordance with s. 45 IPA 2016.

The stored data is admissible before the UK courts and it is subject to the same rules and laws that apply to documentary evidence. There is no specific form required for presenting such data as evidence. Nevertheless, there are guidance notes published by the Association of Chief Police Officers that provide guidance on the identifying, preserving, and recovering of digital evidence.[50] If it can be shown that the stored data was not handled correctly, the accused can challenge the admissibility of that data as evidence.[51]

2. Inadmissibility of evidence as a consequence of inappropriate collection

Electronic communications data obtained other than under an interception warrant would be excluded from use in criminal proceedings under certain circumstances. Under UK law, courts have discretion to exclude prosecution evidence which lacks relevance and which may otherwise endanger the fairness of the trial (s. 78 Police and Criminal Evidence Act 1984). Thus, the defendant can request the exclusion of evidence on the grounds of either the procedure through which evidence was obtained or its reliability. Provided that the defendant's application is rejected and evidence is admitted, the defendant can further challenge evidence during trial by arguing that the standard of proof required for prosecution is not beyond reasonable doubt. These rules on admissibility apply to the evidence gathered under an MLA or a letter of request.

Intercept evidence would also be admissible if it comes from an interception carried out in another country, even though it reveals information about the activities of foreign law enforcement agencies.[52]

---

[50] ACPO Good Practice Guide for Digital Evidence (March 2013), available at https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[51] Section IV.2.

[52] [2004] UKHL 40; [2005] AC 167.

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

1. International conventions

The IPA 2016 contains a specific provision on giving effect to an incoming request or authorising an outgoing request for interception of communications with its mutual assistance warrant regime.[53] There are also a number of international agreements on the exchange of information in criminal matters to which the UK is a party. The EIO Directive was transposed in UK law through the introduction of the Criminal Justice (European Investigation Order) Regulations 2017 on 31 July 2017. The implementation has not yet raised questions about digital evidence. The UK signed the Convention on Cybercrime in November 2001 and ratified in May 2011. The Convention entered into force in September 2011. The UK is also a party to the European Convention on Mutual Assistance in Criminal Matters of 1959 as of 27 November 1991. The UN Transnational Organised Crime Convention of 2000 has been applicable to the UK since its ratification on 9 February 2006 with no reservations. Finally, the UK has opted in to the 2000 EU Convention on Mutual Assistance.

2. Bilateral treaties

The UK has mutual legal assistance treaties (on restraint & confiscation or drug trafficking treaties) with a number of EU Member States (i.e., Italy, Spain, and Sweden). It also has a mutual legal assistance treaty with Ireland. These treaties do not specifically relate to the interception of electronic communication, but rather include provisions on the exchange of information and/or intelligence.

3. National regulation

The Crime (International Co-operation) Act 2003 provides the general framework for mutual assistance in criminal matters including the obtaining of evidence from abroad or assisting overseas authorities with obtaining evidence from the UK. According to this Act, a judge, on the application of a prosecuting authority (e.g., the Crown Prosecution Service) or a person charged in the proceedings (i.e., the defendant), may issue requests for evidence from abroad (ss. 7–12). This request may only be made if an offence has been committed and proceedings for that offence have been instituted, or an investigation is underway (s. 7(1)). The request may be sent to a court in the relevant jurisdiction, to an authority designated in the

---

[53] Section III.B.1.

jurisdiction for receipt of such requests or, in cases of urgency, the International Criminal Police Organisation (s. 8). The evidence, once received, should then only be used for the purpose specified in the request, known as the 'specialty principle' (s. 3(7)). Requests for UK-based evidence by overseas authorities must be sent to the Secretary of State at the Home Office, referred to as the 'territorial authority' (ss. 13–28(9)). The Secretary of State may then nominate a court to receive the requested evidence. As well as achieving the disclosure of particular evidence, the MLA procedure also provides for the obtaining of evidence. The Secretary of State may direct that a warrant be applied for from the courts in order that a search can be undertaken and evidence seized. Law enforcement agencies may also obtain a warrant to intercept communications, as discussed above. However, such coercive powers may only be exercised where the conduct constitutes an appropriate offence in both the requesting country and under the laws of England and Wales, the so-called 'double criminality' principle, as also required in extradition proceedings.

B. Requirements and Procedure (Including the Handling of Privileged Information)

1. Incoming requests

A designated officer as appointed by the Secretary of State may issue interception warrants on the application by the competent authority in accordance with an EU mutual assistance instrument or international mutual assistance agreement (s. 40(2)). These warrants must be for the purpose of obtaining communications relating to (i) a person that appears to be outside the UK; or (ii) the interception required by the warrant is to take place on premises outside the UK (s. 40(1)(a)–(b)). The statutory duty of the telecommunications operator to give effect to the warrant and the rules on unauthorised disclosure also apply to incoming requests for interception as they apply to targeted interception.[54]

Safeguards in relation to obtaining the communications of persons who are Members of Parliament, or privileged materials are applicable to mutual assistance warrants requested by foreign authorities. The IPA 2016 allows for the transfer of copies of the intercepted material to a foreign country, and thus it does not allow for the real-time transmission of that material.

2. Outgoing requests

If a person in the UK asks the authorities of another country or territory to carry out the interception of communications of an individual believed to be in the British Islands at the time of the interception, a targeted interception warrant and tar-

[54] Section III.B.10.

geted examination warrant authorised under the IPA 2016 must be in place (s. 9). Safeguards in relation to the relevant persons of legislative, privileged material, and disclosure and retention of material obtained through the interception apply in this circumstance as well. Where the incoming interception request concerns the obtaining of information about an individual who is believed to be outside the UK, the interception may be carried out by or on behalf of the telecommunications operator if that request is made in accordance with the relevant international agreement by the foreign competent authority (s. 52). The Secretary of State may detail what the relevant international agreements are and the conditions under which the incoming interception may be carried out (ss. 52(3)–(5)). As mentioned earlier, certain safeguards such as those in relation to the disclosure and retention of material and the prohibition of disclosure in legal proceedings outside the UK must be met.[55]

3. Real-time transfer of communication data

As mentioned earlier, the IPA 2016 substantiates mutual legal assistance in relation to the interception of communications with its mutual assistance warrant regime.[56] Therefore, unless there is a mutual assistance warrant issued in accordance with the interception regime under the IPA 2016, the direct interception of communications by foreign authorities (or by the telecommunications operators on behalf of them) would be the criminal offence of unauthorised interception under the same Act.

With regards to the transfer of stored communications data to foreign authorities by UK-based operators, there is no explicit prohibition against that transfer under the IPA 2016. Nevertheless, those operators may be prevented from transferring the data to foreign authorities under the Protection of Trading Interests Act. Section 2 of this Act allows the Secretary of State to direct persons within the UK not to comply with requirements, actual or imminent, by foreign courts, tribunals, or authorities to produce commercial documents or information located outside the territorial jurisdiction of any such authority. In this regard, service providers are prevented from cooperating with foreign authorities if they are asked to produce commercial documents or information.

Another legal basis under which service providers may prevented from such cooperation is UK data protection law. According to the DPA 2018, personal data must not be transferred to a country outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data (s. 18). Therefore, the UK-based operators must transfer of such data in line with its rule on third-country data transfers (ss. 73–76). The DPA 2018 transposes the General

---

[55] IPA 2016, s. 54. See also Section III.B.3.

[56] Section V.B.

Data Protection Regulation in accordance with the European Union (Withdrawal) Act. Thus, once the UK ceases to be a member of the EU, the personal data transfer rules will continue to apply to UK based operators in relation to their cooperation with foreign authorities. Whether those operators would be able to cooperate with the authorities of the remaining EU Member States will depend on how the issue of UK-EU personal data transfer takes shape once the UK leaves the EU.

In order to address the effectiveness of cross-border data sharing, the UK intends to give the UK law enforcement authorities the power to directly access the data stored outside of the UK for the purpose of criminal investigations and prosecutions for serious crimes under the Crime (Overseas Production Order) Bill. The Bill introduces a procedure in which law enforcement authorities and prosecutors would apply for a court order from the UK courts requiring non-UK based service providers to produce or grant access to the communications data sought by the order. The judge may issue an order if they are satisfied that the data is likely to be of substantial value to the criminal proceedings or investigation for which it is being requested, and that it would be in the public interest. Another condition for issuing an overseas production order is that there must be international agreements in place between the UK and the third country in which the service provider is based. To date, the UK has not reached any such agreement with another country, but the negotiations to conclude one with the US continue.

C. European Investigation Order

As mentioned above, the Criminal Justice (European Investigation Order) Regulations 2017 transpose the EIO in UK law. Therefore, if a request is made by an authority in the EU Member State through the EIO regime, that request will be implemented in the UK through those Regulations, rather than the mutual agreement warrant provisions of the IPA 2016.[57]

List of Abbreviations

CMA	Computer Misuse Act
DPA	Data Protection Act 2018
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EHRR	European Human Rights Reports
EIO	European Investigation Order
EWCA	England and Wales Court of Appeal

[57] Section III.B.1.

GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
HRA	Human Rights Act
IOCCO	Interception of Communications Commissioner's Office
IPA	Investigatory Powers Act
IPC	Investigatory Powers Commissioner
ISA	Intelligence Services Act
ISC	Intelligence Services Commissioner
NCA	National Crime Agency
NTAC	National Technical Assistance Centre
OJ	Official Journal of the European Union
OSC	Office of Surveillance Commissioners
RIPA	Regulation of Investigatory Powers Act
UKHL	United Kingdom House of Lords

United States of America*

– Supplementary Report –

National Rapporteur:
Joseph Schwerha

* This report outlines the legislation and case law as of September 2020.

Contents

This article summarizes the ability of governmental authorities to intercept telecommunications, as well as when and how the resultant information can be shared and used with regard to the United States. It is not a comprehensive review and outline of the law and those authorized by the law to intercept telecommunications. Such a survey is beyond the scope of this chapter. Instead, it concentrates on when and under what authority the United States' government may engage in such acts.[1]

I. Overview of Law Enforcement and Security Services with Powers of Telecommunication Interception

The United States government is a constitutional representative republic. It has one federal government and fifty state governments. *National security measures* are reserved almost exclusively for the federal government. *Criminal law enforcement responsibilities* are split between the federal government and the individual states. Moreover, within each state there lie many political subdivisions that have law enforcement authority. Generally, federal authorities are exclusively responsible for prosecuting infractions of the federal penal code and for taking measures to protect national security. Similarly, state law enforcement is usually split between states' attorneys general, which is run at the state government level, and county and city subdivisions, which also prosecute the respective state penal code, albeit only having authority within their respective political subdivision.[2] The federal government has the ability to conduct interceptions for criminal investigations under the Electronic Communications Privacy Act of 1986 (ECPA), as well as, in certain instances, for national security purposes under the Foreign Intelligence Surveillance Act and associated legal authority.[3] This chapter concentrates on federal law enforcement because a thorough review of each state's law on interception is beyond the scope of this volume.

---

[1] I want to thank my research assistant *Scott Conner* for his help in creating this document.

[2] For instance, each county in the state of Pennsylvania has a District Attorney (DA). The DA for each county is responsible for prosecuting criminal offenses that take place in that county, or which other crimes have enough of an effect within their county to give rise to jurisdiction to prosecute same.

[3] See generally 18 U.S.C. §§ 2511 et seq. for the interception authority for criminal investigations.

II. Powers to Intercept Communication under Criminal Procedure

A. Introduction

1. Respective laws and courts

In the United States, the federal court system is in charge of resolving disputes involving both civil and criminal wrongs. In order to preserve the rights of litigants, the federal courts follow either the Federal Rules of Civil Procedure or the Federal Rules of Criminal Procedure, depending upon what kind of dispute presently is before the court. The admissibility and use of evidence in court proceedings is governed by the Federal Rules of Evidence.[4]

The Federal Rules of Criminal Procedure are promulgated by the United States Supreme Court pursuant to the Rules Enabling Act.[5, 6] While these rules apply to all criminal proceedings in federal court, in certain cases they can also apply to state court proceedings. The Rules of Criminal Procedure have no real effect on the laws of national security, except when someone operating under the rules of national security commits a criminal act.

The United States does not have a singular law or legal theory that generally protects personal data. This is quite the opposite to the European Union with its General Data Protection Regulation. Instead, the United States has an implied right to privacy derived from the United States Constitution, along with a variety of federal laws protecting privacy in certain areas. In addition, every state has additional laws which protect the privacy rights of its citizens in distinct areas.[7]

2. Civil and human rights safeguards under constitutional and criminal procedural law

With regard to the rule of law concerning real-time interception, the most critical statutes are the ECPA (Electronic Communications Privacy Act) and the FISA (Foreign Intelligence Surveillance Act). Both statutes enforce privacy for both the nation and individual citizens. These pieces of legislation focus on different aspects of the law. The ECPA governs crime and intrusions among citizens, and FISA primarily deals with national security measures.

---

[4] See the Federal Rules of Evidence.

[5] See 28 U.S.C. §§ 2072 and 2074.

[6] These rules are initially drafted by the Advisory Committee to the Judicial Conference of the United States, and then, after comments, are submitted to the Standing Committee on Rules of Practice and Procedure, which then submits them to the Judicial Conference, who then submits them to the U.S. Supreme Court for approval.

B. Background and Historical Development

Conventional eavesdropping was not a severe crime in early American times. Following the advent of the telegraph and the telephone, state law played a more visible role in proscribing wiretapping or any telephone indiscretions by phone and telegraph operators. The first wiretap statute was put in place to protect government secrets during World War I. Subsequent legislation outlawed the divulging of private radio messages through the 1927 Radio Act, without the enactment of federal wiretap prohibitions. Up until the iconic Olmstead Supreme Court decision in 1928, most states – forty-one of the forty-eight – had laws protecting private telephone and telegraph information.

Olmstead[8] was a bootlegger who contested his conviction as a violation of his Fourth and Fifth Amendment rights regarding self-incrimination, citing the wiretapping as the primary malfeasance by the government. In the ruling, Chief Justice Taft expressed the duty of Congress to protect individuals where the Constitution fell short. The Olmstead decision is remembered mostly for the proposition that there can be no violation of the Fourth Amendment for government wiretapping without actual physical trespass upon the subject's property.

The idea that violations could include the overhearing of verbal statements gave a broader perspective of the rights under the Fourth Amendment. Individual states set up a system defining the acquisition of a warrant or court order of similar capacity for an authorized wiretap or any form of electronic eavesdropping to alleviate the hurdles encountered throughout obtaining information. The courts determined the state statutory schemes as constitutionally inadequate in 1967 in *Berger v. New York*[9] due to the lack of provisions requiring:

- the proper description of the place subjected to a search,
- a comprehensive outline of the crime necessitating the search,
- definitive details of the conversation subject to seizure,
- limitations aimed at keeping general searches in check,
- mechanisms to terminate interceptions once the material of interest is acquired,
- timely execution of the acquisition,
- an account of seized items,
- the evidence of pressing situations that overrule the need for prior notice.

Berger subsequently led to the enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. This Act was a comprehensive statute outlawing both wiretapping and electronic eavesdropping.

---

[8] *Olmstead v. United States*, 277 U.S. 438 (1928).

[9] 388 U.S 41 (1967).

The need for wiretapping and electronic eavesdropping through a court-supervised procedure came about as a result of another Supreme Court case. This process ultimately brought about the FISA (Foreign Intelligence Security Act) in 1978. The FISA governs all information gathering procedures for foreign intelligence purposes. The issue of inherent presidential power as the basis of a wiretap – in the absence of judicial approval – based purely on internal threats to national security[10] remained unaddressed, and as a result, the issue was struck off the Title III scheme.

United States v. Miller[11] established the absence of Fourth Amendment protection expectations for a client regarding privacy of records detailing transactions with a financial institution. Government access is allowed with issuance of a subpoena duces tecum,[12] deemed more comprehensive than a general warrant.

The consensus of the court in *Smith v. Maryland*[13] was that a warrant is not necessary for information acquired by telephone companies for regular billing procedures. The court decided that a permit is not required to legalize the state's use of pen registers[14] or trap and trace equipment.

Congress enacted the ECPA in 1986. The statute comprises of three parts:

– The revised Title III;[15]
– The Stored Communications Act (SCA);[16]
– Legal provisions for installation and use of tap and trace equipment and pen registers.[17]

Legislation has been enacted to augment the ECPA and FISA, and prominent among these are:

– The USA Patriot Act (2001);
– The Department of Homeland Security Act (2002);
– The 21st Century Department of Justice Appropriations Authorization Act (2002);
– The Intelligence Authorization Act for Fiscal Year 2002 (2001);
– The USA PATRIOT Improvement and Reauthorization Act (2006);
– The Foreign Intelligence Surveillance Act of 1978 Amendments of 2008 (2008).

---

10 *United States v. United States District Court,* 407 U.S 297 (1972).
11 425 U.S 435, 441–443 (1976).
12 This is an order for the recipient to come and produce certain identified documents.
13 442 U.S 735, 741–746.
14 See section II.E. below.
15 18 U.S.C. §§ 2510–2522.
16 18 U.S.C. §§ 2701–2712.
17 18 U.S.C. §§ 3121–3126.

C. Lawful Interception

1. Prohibitions

It is a crime to engage in wiretapping or alternative forms of electronic eavesdropping, as well as to possess the equipment meant to facilitate the same.[18, 19] At the heart of the ECPA is the prohibition of illegal wiretapping and electronic eavesdropping.[20] Specifically, 18 U.S.C. § 2511 prohibits any person[21] from intentionally intercepting, or endeavoring to intercept a wire, electronic or electronic communication by using an electronic, mechanical or like device.[22] However, it is not a crime if the conduct is specifically authorized or expressly not covered.[23]

---

[18] 18 U.S.C. § 2511.

[19] The disclosure of sensitive information obtained through a court order is a federal offence, 18 U.S.C § 2511.

[20] Please note that there are separate crimes for associated activities, including but not limited to: illegal use of a pen register or trap and trace device, 18 U.S.C. § 3121, as well as illegal access to stored communications, 18 U.S.C. § 2701.

[21] By definition in the statute, a person is: any employee, or United States agent, or a representative of any State or recognized political subdivision, or any individual, partnership, joint stock company, corporation, trust, or association, 18 U.S.C 2510(6).

[22] See 18 U.S.C. § 2511, "(1) Except as otherwise specifically provided in this chapter any person who--

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when-

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained

There is also a general provision against using or disclosing information obtained in violation of this prohibition.[24] Indeed, it is a crime to even endeavor to do so.[25] These proscriptions likewise apply to possession or trafficking in devices which have the primary purpose of engaging in such illegal wiretapping or eavesdropping.[26]

In legislation, interception is acquisition of content in real-time of private communication with the aid of electronic equipment. Access of material after the acquisition of information does not amount to interception.[27] Inadvertent conduct is not a crime, and one must have acted with intent to break established law, with knowledge of the relevant legal provisions.

2. Lawful interception requirements

a) General requirements

Federal and state law enforcement officials are exempt from these proscriptions under three circumstances:

1. pursuant to a valid court order;
2. with the consent of one of the parties to the real-time communication; or
3. regarding communications of someone who is illegally intruding into a communications system.

At the federal level, to secure a valid interception order in a federal criminal investigation a senior US Department of Justice official must approve the application

---

through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation."

[23] For example, there is no crime, if: 1. One of the parties authorized the interception, 2. the interception occurs in compliance with a judicially authorized interception, 3. the interception occurs as part of regulating or providing communication services, 4. certain radio broadcasts, or 5. in certain cases regarding spouses who are intercepting. See Stevens and Doyle, Privacy: An Abbreviated Outline of Federal Statutes Governing Wiretapping and Electronic Eavesdropping, Congressional Research Service (9 October 2012).

[24] See 18 U.S.C. § 2511.

[25] Id.

[26] 18 U.S.C. § 2512.

[27] The USA PATRIOT Act broadened the uncertainty about voicemail to include stored wire communications coverage, 18 U.S.C § 2703.

for the court order for wire or oral communications.[28] This procedure is only available if the order contains evidence that one of a long list of predicate offenses has been committed,[29] or the whereabouts of someone fleeing from prosecution of one of these offenses.[30] However, any federal prosecutor may approve an application for real-time interception of email or other electronic communications.[31] At the state level, the highest prosecutor in each state or any of its political subdivisions may approve the application for wiretapping or electronic eavesdropping if such order contains evidence of a felony under state law of murder, drug trafficking, kidnapping, robbery, gambling, child sexual exploitation, child pornography, bribery, extortion, or any other crime dangerous to life, liberty and property.[32]

All of the aforesaid applications must include the following elements:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.[33]

In order for the judge of competent jurisdiction to authorize any of the above applications, they must find:

---

[28] 18 U.S.C. § 2516(1).

[29] 18 U.S.C. § 2518.

[30] Id.

[31] 18 U.S.C. § 2515(1)(l).

[32] 18 U.S.C. § 2516(2).

[33] 18 U.S.C. § 2518(1)(a–f).

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.[34]

There are further requirements set forth for the orders themselves, which must include:

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.[35]

Further, the order must be limited by time, requiring that the order contain provisions that said order be executed as soon as practicable and in such a way that will minimize the capture of innocent communications.[36] And if requested, said orders can include specific direction that the communications providers, as well as parties necessary for the execution of the order cooperate in the execution of the order.[37]

b) Special privileges for specific professions and sensitive information

American common law and many, if not all states have explicitly recognized that certain information may not be utilized or even read due to those communications being privileged. There are four basic privileges available under both federal and state[38] law: 1. attorney-client privilege,[39] 2. clergy-communicant privilege,[40] 3. doc-

---

[34] 18 U.S.C. § 2518(3).

[35] 18 U.S.C. § 2518(4).

[36] 18 U.S.C. § 2518(5).

[37] Id. Note that these procedures can be postponed until after the interception has begun upon approval of senior U.S. Department of Justice officials in certain cases involving death or serious injury, 18 U.S.C. § 2718(7).

[38] Please note that a full review of each state's law within the U.S. is beyond the scope of this article.

tor-patient privilege,[41] and 4. marital communications privilege.[42] Generally, four fundamental elements must be present for a privilege to attach to a communication:

> "1) the communications must be made with the belief that they will not be disclosed; 2) confidentiality must be essential to the relationship between the parties; 3) the relation between the parties must be one that the community seeks to encourage and protect, and; 4) the injury caused by the disclosure of the communication must be greater than the benefit gained by disclosure for justice."[43]

Finding these elements present, courts have then long recognized the privilege in certain communications between attorneys and their clients, clergy and their followers, wives and husbands, and doctors and their patients.[44] The first two are integrally related to the United States Constitution. The attorney-client privilege is supported by the Sixth Amendment to the United States Constitution, which guarantees that every person who is accused of a crime has the right to legal counsel.[45] The clergy-communicant privilege is supported by the First Amendment to the United States Constitution, which guarantees freedom of religion.[46]

aa) Prohibition of use of privileged communications

Lawful surveillance has the primary purpose of assisting in certain investigations, as long as the extensive list of prerequisites can be met.[47] However, just because a communication is legally surveilled, this does not mean that those communications can be listened to or otherwise used by the persons doing the investigation. While the U.S. Code authorizes use of properly intercepted communications by investigative or law enforcement officers, it explicitly prohibits use of privileged communications.[48] It does so plainly: "[n]o otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the

---

[39] See *Fisher v. United States*, 425 U.S. 391, 403 (1976). See also M. Winick, B. Burris, and Y. Bush, Playing I Spy with Client Confidences: Confidentiality, Privilege and Electronic Communications, 31 Tex. Tech L. Rev. 1225, 1229 (2000).

[40] See *Totten v. United States*, 92 U.S. 105, 107 (1875).

[41] See *Simpson v. Braider*, 104 F.R.D. 512, 522 (D.C. Cir. 1985).

[42] See *Trammel v. United States*, 445 U.S. 40, 50 (1980); T. Kossegi & B. Phair, The Clergy-Communicant Privilege in the Age of Electronic Surveillance, Journal of Civil.

[43] Id. at 244, citing John H. Wigmore, Wigmore on evidence § 2285 (McNaughton rev. ed. 1961).

[44] Id. at 244–245.

[45] Id. at 249.

[46] Id. at 249–250. Please note that there are many other recognized privileges that will not be discussed here. See L. Gray, Evidentiary Privileges, 6th ed. (Grand Jury, Criminal and Civil Trials) (accessed on 30 September 2020 at https://nysba.org/NYSBA/Publications/Books/TOCs and Author Bios/40996_Evidentiary6th.pdf).

[47] See above II.C.2.a).

[48] See 18 U.S.C. § 2517(4).

provisions of this chapter shall lose its privileged character."[49, 50] However, please note that while privileged communications may not be used, the mere fact that a certain communication may be privileged does not prohibit it from being intercepted.[51] Moreover, there are exceptions to privileges. For example, the crime-fraud exception to the attorney-client privilege is widely known. This removes the protection of "the attorney-client privilege for communications concerning contemplated or continuing illegal or fraudulent acts."[52]

bb) Minimization

Under the ECPA, "[e]very order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter."[53] Thus, efforts must be made to minimize interception of communications that the government was not authorized to use, which has been argued to include privileged communications.[54]

cc) Procedures implemented to protect privileges at the federal level

Since authorities know that certain targets are more likely than others to have a significant amount of privileged communications (i.e., attorneys in public corruption cases), prosecuting authorities normally would take precautions to avoid inadvertently listening to privileged communications. One common way would be to set up a "taint team" to do the initial listening to the wiretapped communications.[55] They then would decide what communications were pertinent and non-privileged and only subsequently let those communications be used by the prosecutors and investigators in the actual case. Ideally, then, the taint team never communicates with the actual investigators and prosecutors.

This method is criticized for placing too much discretion with the investigative authorities while providing too little actual protection against disclosure to the gov-

---

[49] Id.

[50] See also Electronic Surveillance Manual, Procedures and Case Law, Forms, Electronic Surveillance Unit, Office of Enforcement Operations, Criminal Division, U.S. Department of Justice (June 2005).

[51] See Kosseg & Phair at 253.

[52] R. Strassberg and M. Splillane, Privilege: The US Perspective, 36.1 Privilege in law enforcement investigations, 3 January 2020 (accessed on 30 September 2020 at https://globalinvestigationsreview.com/benchmarking/the-practitioner's-guide-to-global-investigations-fourth-edition/1212402/privilege-the-us-perspective).

[53] See 18 U.S.C. § 2518(5).

[54] See Kosseg & Phair at 253.

[55] This is sometimes referred to as a "Chinese wall" in civil litigation.

ernment, even if it is a supposedly totally separate team.[56] Indeed, there are fair arguments on both sides. For example, assume a target is talking to his attorney about proper ways to lessen his income tax burden from monies he has from a business practice that the investigative authorities claim is criminal in nature due to his questionable representations to investors. Instead of the taint team eliminating those communications as privileged, they allow investigators to use the same, claiming that the conversations involved show a plan for future criminal activity, which would remove them from being privileged. The investigators get access to those communications and utilize them and numerous other pieces of evidence to prosecute the target. In pretrial motions, the now defendant seeks to suppress those conversations. Even if successful, it would be very hard to now remove all influence of those conversations from the investigators' minds. On the other hand, what other methods would allow for investigations and provide better protections?[57] In the end, the potential (and evidence) of abuse[58] may support a quest for real reform.

ee) Waiver of privilege

Under both federal and states' laws, the holder of a valid privilege may waive that privilege.[59] Generally, the privilege can only be waived by the person who possesses the privilege, and the procedure for waiver may be different depending upon the exact type of privilege. Of course, the privilege can be waived directly and knowingly by the person possessing same.[60] The waiver goes to not only that communication, but also to other communications relating to the same matter.[61]

---

[56] See Government "'Taint Teams' May Open a Pandora's Box: Protecting Your Electronic Records in the Event of an Investigation," WilmerHale Blog, 2004-05-11 (accessed on 30 September 2020 at https://www.wilmerhale.com/en/insights/publications/government-taint-teams-may-open-a-pandoras-box-protecting-your-electronic-records-in-the-event-of-an-investigation-may-11-2004).

[57] These taint teams can also be used for pen/trap operations, as was reportedly done in the Michael Cohen investigation. See C. Kalmbacher, Here's How the Feds (Tried to) Keep Attorney-Client Privilege Intact During Cohen Wiretaps, Law & Crime blog, 3 May 2018 (accessed 30 September 2020 at https://lawandcrime.com/uncategorized/heres-how-the-feds-kept-attorney-client-privilege-intact-during-the-cohen-wiretaps/amp/).

[58] See S. Baker, Partisan Taint in the Trump-Russia Investigation, Lawfare blog (8 September 2020) (accessed 30 September 2020 at https://www.lawfareblog.com/partisan-taint-trump-russia-investigation).

[59] Please note that we concentrate our analysis of privilege on merely those likely to be held by a potential defendant in a criminal investigation. This analysis summarizes the most popular privileges only. It does not purport to be a comprehensive analysis of all privileges available under state or federal law. For example, we will not discuss the presidential communications privilege, the bank examination privilege nor the state secret privilege.

[60] See Enforcement Manual, Commodity Futures Trading Commission, p. 44 (20 May 2020).

[61] R. Strassberg and M. Splillane, Privilege: The US Perspective, 36.1 Privilege in law enforcement investigations, 3 January 2020 (accessed on 30 September 2020 at

However, the privilege may also be waived inadvertently,[62] or carelessly by allowing a non-privileged party to have access to said communication. And while all fifty states have wiretap statutes, the restrictions for lawful interception can be heightened; however, they cannot be lower than those present under the ECPA.[63] Indeed, numerous states go further and prohibit both the interception and the use of privileged communications.[64]

ff) Inadvertent waiver

Under Federal Rule of Evidence 502(b), a person who discloses information covered by the attorney-client privilege or work-product privilege "in a federal proceeding or to a federal office or agency" does not waive that privilege if:

(1) the disclosure is inadvertent;

(2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and

(3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26 (b)(5)(B).[65]

Of course, this mostly applies to documentary evidence and is considered here for the circumstance where waiver occurred outside of the wiretapped communications but that the waiver operates to allow listening in to communications, the subject matter of which had already been waived.

c) Time limitations

The above-mentioned court orders must be in force only for as long as necessary, but not more than thirty days.[66] However, additional thirty day extensions may be granted if the requirements of the original application are still met, though the court may require updates more frequently than every thirty days.[67]

---

https://globalinvestigationsreview.com/benchmarking/the-practitioner's-guide-to-global-investigations-fourth-edition/1212402/privilege-the-us-perspective).

[62] See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009). Available at: https://repository.law.umich.edu/mlr/vol107/iss4/1 (illustrating how someone could inadvertently waive privilege by placing a technical communication through a third party).

[63] Id.

[64] Id. (stating that thirteen states and the District of Columbia fell into that category at the time that article was written).

[65] See Fed. R. Evid. 502.

[66] 18 U.S.C. § 2518(5).

[67] 18 U.S.C. § 2518(6).

d) Notice, security, and sharing requirements

All intercepted communications are to be recorded and the evidence secured and placed under seal, along with the application. Within ninety days of the expiration of the order, those individuals whose communications were intercepted are entitled to notice.[68]

There are strict restrictions on how, by whom or to whom the information derived from the court order may be disclosed or used, including rules with regard to disclosure by or to:

1. other law enforcement officers,[69]
2. foreign officials,[70]
3. federal intelligence officers when involving foreign intelligence information,[71]
4. other federal officials, or foreign government officials involving hostile acts of a foreign power,[72] and
5. witnesses testifying in state or federal proceedings.[73]

3. Consequences of an illegal interception

a) Criminal and civil liability

If one does illegally intercept, use or disclose communications in violation of Title III, this is punishable by imprisonment of not more than five years and not more than a $250,000 fine.[74] This also applies to cell phone communications and cordless communications. Intercepting satellite communications has a reduced penalty, as long as it is not conducted for tortious, criminal or like purposes.[75]

There is also civil liability for violations. Victims of a violation of Title III, can be entitled to equitable relief, damages (equal to the greater of $100 per day of violation, or $10,000). If successful, victims can recover punitive damages, attorney's fees and/or litigation costs. Depending upon the court, this could be mandatory or discretionary.[76] Even the United States may be directly liable for willful violations

---

68 18 U.S.C. § 2518(d).

69 18 U.S.C. § 2517(1), (2) and (5).

70 18 U.S.C. § 2517(7).

71 18 U.S.C. § 2517(6).

72 18 U.S.C. § 2517(8).

73 18 U.S.C. § 2517(3) and (5). Note that ten days notice must be given to those people whose communications were intercepted and provided the intercepted communications are not privileged. See 18 U.S.C. § 2518(9) and 18 U.S.C. § 2517(4).

74 18 U.S.C. § 2511(4)(a).

75 18 U.S.C. § 2511(4)(b).

76 18 U.S.C. § 2520(b) and (c).

of the Foreign Intelligence Surveillance Act and/or the Stored Communications Act.[77]

b) Evidentiary consequences

If evidence of any sort is illegally obtained, the subject's civil rights are protected because such evidence cannot legally be admitted in any criminal prosecution due to the Exclusionary Rule. To summarize, any evidence directly illegally obtained or that is derived from that illegally obtained evidence shall not be admitted into evidence in any criminal proceedings against the individual it applies to.

ECPA explicitly provides additional protections under Section 2515, but only for wire and oral communications. That section provides:

> [w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.[78]

In practice, any such aggrieved person "may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that:

> (i) the communication was unlawfully intercepted;
>
> (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
>
> (iii) the interception was not made in conformity with the order of authorization or approval.[79]

Mere technical violations will not be sufficient.[80]

D. Stored Communications

1. General access to stored communication under 18 U.S.C. §§ 2701–2712

In general, it is illegal for someone to obtain access to electronic communication while in storage without authorization or in excess of their existing authorization.[81] Likewise, the providers of "electronic communication services" and "remote com-

---

[77] See 18 U.S.C. §§ 2701–2712. If successful, plaintiffs can recover actual damages, $10,000 and litigation costs.

[78] 18 U.S.C. § 2515.

[79] See 18 U.S.C. § 2518(10).

[80] See *United States v. Lomeli*, 676 F.2d 734, 739 (8th Cir. 2012).

[81] 18 U.S.C. § 2701.

puting services" may not voluntarily disclose the contents of communications on those services to any person or entity.[82]

It is easier for governmental entities to obtain already received stored electronic communications and transactional records than to acquire live intercepts. However, the law surrounding stored electronic communications is equally complicated, and is contained within 18 U.S.C. §§ 2701–2712. In general, law enforcement officials are entitled to access stored communications:

1. with consent of one of the parties,[83]
2. with respect to the court order or similar process established by the ECPA,[84]
3. in some emergency situations involving death or serious bodily injury,[85] or
4. under one of the other statutory exceptions to the ban against disclosure.[86]

---

[82] 18 U.S.C. § 2702(a).

[83] 18 U.S.C. § 2702(b)(3) and (c)(2).

[84] 18 U.S.C. § 2702(b)(2) and (c)(1).

[85] 18 U.S.C. § 2702(b)(7) and (c)(4).

[86] See 18 U.S.C. § 2702(b):

"(b) Exceptions for disclosure of communications.—A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub. L. 108–21, title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency; or

(9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(c) Exceptions for Disclosure of Customer Records.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

Section 2702 gives different protections to the content of stored wire and electronic communications depending upon how long the communications have been in electronic storage. The government must use a search warrant to access the material if it has been in electronic storage for less than 180 days.[87] This same procedure must be used for older communications or those in remote computer storage if no notice of such access would be given to a subscriber or customer. However, if the government is willing to provide notice, even delayed notice, then access to the data may be had with an order that merely satisfies the standard that the information obtained is relevant and material to a criminal investigation.[88]

2. Access to specific traffic data under 18 U.S.C. § 2703

Under Section 2703, the government may compel information in the possession of the electronic communication service or remote computing services. Specifically:

> [a] provider of electronic communication service or remote computing service shall disclose to a governmental entity the
>
> (A) name;
>
> (B) address;
>
> (C) local and long distance telephone connection records, or records of session times and durations;
>
> (D) length of service (including start date) and types of service utilized;
>
> (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
>
> (F) means and source of payment for such service (including any credit card or bank account number).

These can be obtained using several different legal processes.[89]

---

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(6) to any person other than a governmental entity; or

(7) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523."

[87] 18 U.S.C. § 2703(a).

[88] 18 U.S.C. § 2703(b). Note that this can also be obtained pursuant to administrative subpoena, grand jury subpoena, trial subpoena or court order.

[89] 18 U.S.C. § 2703.

If the governmental entity is compelling revelation of information under Section 2703 through a court order, said entity can delay notification of the person to whom such data pertains for a 90 day period where giving notice would produce an "adverse result", which would include:

1. endangering the life or physical safety of an individual,
2. flight from prosecution,
3. tampering with evidence,
4. intimidation of witnesses, or
5. otherwise seriously impeding an investigation or unduly delaying a trial.[90]

If the government is attempting to obtain information other than the content of communications, then such information can be obtained with any of the following: a warrant, a court order, with customer consent, with a written request in telemarketing fraud cases or with a subpoena in certain cases.[91] In such cases, the information can be obtained without providing notice to the individual to whom the information applies.[92]

3. Consequences under the Stored Communications Act

The Exclusionary Rule's protections do not stop at interception of real-time communications. Even transmissions that have been received are protected from illegal use after they have reached their destinations. The Stored Communications Act (SCA) thereby provides protection against unauthorized access to communications that have been received or are in temporary intermediate storage.[93]

Accordingly, the ECPA, in the Stored Communications Act, bans surreptitious access to communications at rest, although it does so beyond the confines that apply to interception, 18 U.S.C. §§ 2701–2711:

> [g]eneral proscription makes it a federal crime to:
> – intentionally either access without authorization or exceed an authorization to access
> – a facility through which an electronic communication service is provided
> – and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.[94]

---

[90] 18 U.S.C. § 2705(a)(2) and (b).

[91] 18 U.S.C. § 2703(c).

[92] 18 U.S.C. § 2703(c)(3).

[93] See 18 U.S.C. §§ 2701–2711.

[94] See Stevens and Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electric Eavesdropping*, Congressional Research Service, (9 October 2012), citing, 18 U.S.C. § 2701(a).

This prohibition has three basic elements: "access, to a facility through which service is supplied, and consequences (obtain, alter, prevent access to a wire or electronic communication)."[95]

E. Capturing of Traffic Data (Pen Registers and Trap and Trace Devices)

1. Definition

A pen register is any device that can record and decode dialling, routing, addressing, or signalling information which reveals the recipient of the communication; a trap and trace device captures and decodes incoming signals that identify the source of communication.[96] That statute specifically defines a pen register as: "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication."[97] It goes on to define a trap and trace device as: "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication."[98] Pen registers and trap and trace devices have a distinct role in surveillance law. These devices do not expose the contents of communications. Instead, these devices are limited to showing the source or recipient of a communication signal.

2. Prohibitions

It is fundamental that pen registers and trap and trace devices do not reveal any contents of the communications they intercept. The moment any device does so, it is subject to Title III wiretap provisions.[99] Next, there is the general prohibition against the use of pen registers and trap and trace devices unless one of the exceptions are met. First, a device may only be used pursuant to a court order under 18 U.S.C.A. § 3123 or under the Foreign Intelligence Surveillance Act (FISA).[100] Second, service providers are granted further exceptions for their use of such de-

---

95 Id.

96 18 U.S.C.A. § 3127(3), (4).

97 18 U.S.C.A. § 3127(3).

98 18 U.S.C.A. § 3127(4).

99 See 18 U.S.C.A. § 2518.

100 18 U.S.C.A. § 3121(a).

vices: when incidental to the providing of service; when needed to protect users from abuse; when needed to protect the provider from abuse; or when the user consents.[101] Lastly, there is an exception for emergency situations outlined in 18 U.S.C.A. § 3125(a).

3. Government access

Federal government attorneys and state and local police officers must apply for a court order to authorize the installation and use of pen registers and trap and trace devices. To do so, they must certify that the device will provide information relevant to a pending criminal investigation.[102] The application must also be made to "a court of competent jurisdiction" over the offence being investigated.[103]

The emergency exception under 18 U.S.C.A. § 3125 allows senior Justice Department or state prosecutors to use pen registers and trap and trace devices before receiving court approval. This exception applies to cases that involve: immediate danger of death or serious injury; organized crime conspiracy; threats to national security; or an attack on a protected computer.[104] The emergency doctrine only gives the government a 48-hour window. If a court denies the application or does not approve it within 48 hours, the surveillance must cease.[105]

4. Consequences

The unauthorized use of pen registers and trap and trace devices is a federal crime, punishable by imprisonment for not more than a year and/or a fine of not more than $100,000 ($200,000 for an organization).[106] There is, however, no exclusionary rule for violations. Therefore, even if the statute is violated it is not a basis to exclude the resulting evidence.[107]

18 U.S.C.A. § 3124(e) outlines a good faith defense to violations. One may argue that their actions were a good faith reliance "on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, [or] a statutory authorization."[108]

---

101 18 U.S.C.A. § 3121(b).

102 18 U.S.C.A. § 3122.

103 Id., see 18 U.S.C.A. § 3127(2).

104 18 U.S.C.A. § 3125(a)(1).

105 18 U.S.C.A. § 3125(b).

106 18 U.S.C. §§ 3121(d), 3571.

107 Gina Stevens & Charles Doyle, Cong. Research Serv., 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping* 49 (2012).

108 18 U.S.C.A. § 3124(e).

G. Duties of Telecommunications Providers to Cooperate

1. Background

The Communication Assistance for Law Enforcement Act (CALEA), also known as "Digital Telephony Act," is a wiretapping law passed by the United States in 1994.[109] The purpose of the Act is to enhance the ability of law enforcement and intelligence agencies to conduct electronic surveillance.[110] The law requires telecom operators and telecom equipment manufacturers to modify and design their equipment, facilities, and services to ensure they have monitoring capabilities that allow federal agencies to monitor all telephony, broadband internet, and VoIP communications in real time.

The US surveillance and intelligence system has a long history founded in the Fourth Amendment to the US Constitution, the Federal Communications Act of 1934, and the Comprehensive Crime Control and Street Safety Act of 1968. However, the rapid spread and development of new technologies has brought severe challenges, and the traditional methods of investigation could no longer fulfill the powers granted in previous acts.[111]

2. CALEA 1994: general requirements

Since 1970, the US communications industry has been asked to work with law enforcement agencies to assist them in electronic surveillance. The development of digital technology and internet services dramatically challenged the law enforcement agencies' monitoring actions. Under the efforts of the FBI, in October 1994, the US Congress passed the CALEA.

The CALEA applies to telecommunications carriers.[112] Telecommunications carriers are defined as entities engaged in the transmission of communications as a common carrier including providing commercial mobile service or such services that act as a replacement for a substantial portion of the local telephone exchange service.[113] The CALEA requirements ensure that telecommunications carriers are capable of: 1) isolating specified communications and enabling the government to intercept communications; 2) isolating specified call-identifying information and enabling the government to access call-identifying information that is reasonably available to the carrier; 3) delivering intercepted communications and call-identi-

---

[109] CommPub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in sections of 18 U.S.C. and 47 U.S.C. (2018)).

[110] Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279, at preamble (1994).

[111] 140 CONG. REC. H10773-02, H10780 (Oct. 4, 1994) (statement of Rep. Markey).

[112] 47 U.S.C. § 1002(a)(2018).

[113] 47 U.S.C. § 1001(8)(2018).

fying information to the government.[114] Telecommunications carriers will be required to perform these actions pursuant to a court order or other lawful authorization.[115] Such orders must be carried out on a confidential basis.

If a carrier fails to comply with the requirement, the court may apply the enforcement measures presented in 18 U.S.C § 2522.[116] This section allows a court to impose a civil penalty of up to $10,000 per day for each day in violation.[117]

3. CALEA 2004: expansion to include new technologies

In 2004, the DOJ, FBI, and DEA filed a joint petition to expand the coverage of CALEA to cover voice-over-IP (VoIP) services and broadband internet access services.[118] The FCC adopted this measure and issued its First and Second Report and Order to implement and outline the expansion.[119, 120] This expansion was viewed as a fulfilment of CALEA's inclusion of services that functionally replace phone and transmission services.[121]

4. Recent requests to expand

a) Providing backdoors

The FBI has continued to push for broader application of the CALEA. Technology has not ceased to progress, therefore the argument that the law must broaden to account for changes remains applicable. Beginning in 2010, the FBI argued that all instant messaging services should have a backdoor for the government to keep suspects from "going dark."[122] The FBI has also proposed fining companies that do not program this backdoor into their services.[123] These measures have not yet been added to the CALEA.

---

114 47 U.S.C. § 1002(a) (2018).

115 Id.

116 47 U.S.C. § 1007(a) (2018).

117 18 U.S.C § 2522(c) (2018).

118 Joint Petition for Expedited Rulemaking, RM-10865 (filed 10 March 2004) (DOJ Petition).

119 *Communications Assistance for Law Enforcement Act and Broadband Access and Services, First Report and Order and Further Notice of Proposed Rulemaking*, 20 FCC Rcd 14989 (2005).

120 *Communications Assistance for Law Enforcement Act and Broadband Access and Services, Second Report and Order and Memorandum Opinion and Order*, 21 FCC Rcd 5360 (2006).

121 20 FCC Rcd 14989, para. 13 (2005).

122 Charlie Savage, U.S. Weighs Wide Overhaul of Wiretap Laws, 2013, https://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html?ref=charliesavage (last visited 8 January 2019).

123 Id.

b) Decryption obligations

Currently, there is no recognized duty for communications providers, or even device manufacturers, to decrypt web-based communication applications or even devices used for telecommunications.[124] While CALEA sets forth the obligations of telecommunications providers, those obligations have yet to be extended to web-based communication applications. This controversy is still very current. It appears that the Federal Bureau of Investigation has attempted to have Facebook held in contempt of court for failing to decrypt Facebook Messenger voice communications and thereby failing to cooperate with an investigation. While the case was sealed, it has been reported in national services that the court sided with Facebook on or about 29 September 2018.[125]

H. Statistics on Use of Government Authorized Intercepts

The United States provides for both federal and state governments to engage in legally authorized intercepts, but most federal and state laws also have provisions that mandate reporting of the use of intercepts. The United States federal court system keeps an annual report of intercepts applied for under US criminal law.[126] As reported, the US federal government, the District of Columbia, the Virgin Islands, and 44 states have laws that authorize courts to approve wire, oral, and electronic surveillance.[127]

The most recent report was last updated on 31 December 2019.[128] It notes that federal and state wiretaps increased by 10 % from 2018 to 2019.[129] In 2019, there were a total of 3,225 wiretaps authorized, with 1,417 being authorized by federal judges. There was a decrease of 3 percent in authorizations by federal court judges while state court judges' authorizations showed an increase of 21 percent.[130]

Having 50 different states, each containing many different jurisdictions (i.e., cities, counties, and judicial districts), there were intercept authorizations spread

---

[124] In 2016, there was a significant dispute between the Federal Bureau of Investigation and Apple regarding the contents of an iPhone belonging to a person involved with the alleged murder of government employees in the state of California. That case was never resolved by the Court because the FBI found a contractor that could decrypt the telephone.

[125] See Crocker and Cardozo, Don't Shoot the Messenger, EFF, 23 August 2018 (https://www.eff.org/deeplinks/2018/08/dont-shoot-messenger).

[126] See United States Courts Wiretap Report 2019 (accessed 29 September 2020 at https://www.uscourts.gov/statistics-reports/wiretap-report-2019).

[127] Id.

[128] Id.

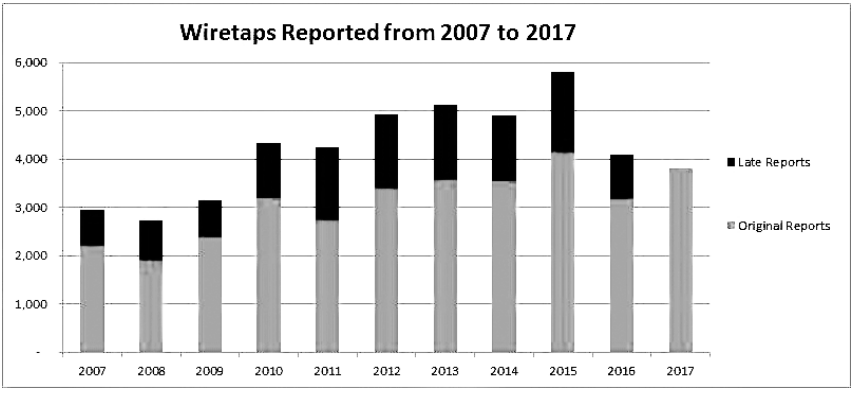
[129] Id.

[130] Id.

across the United States at the state level. In fact, intercepts were authorized by 147 separate jurisdictions, while 79 percent were concentrated in six states.[131, 132]

The reporting provides not only the number of approved applications but it also gives an indication of the time period of each intercept authorization.[133] Federal and state laws in the United States provide for a standard time period limitation of 30 days. However, that time period can be extended one or more times with court approval. The average reported extension was 30 days, with 2,528 extensions having been authorized in 2019.[134] The longest time period for a federal intercept authorization that was terminated in 2019 was extended 27 times for a total of 756 days.[135] The most common subject of these orders was a "portable device,"[136] which includes cell phone communications and apps. In fact, 94 percent of all authorized wiretaps in 2019 were for portable devices.[137]

Since these statistics are mandated, there is data available from several years. The following graph represents wiretaps reported from 2007 to 2017:[138]



131 See id. (California, Colorado, New York, Nevada, North Carolina, Pennsylvania). New York accounted for 28 % of all state approved applications.

132 See id. for graph.

133 Id.

134 Id.

135 Id. (describing wiretap order issued in the District of Arizona, reportedly for a narcotics investigation).

136 Id.

137 Id.

138 Id.

III. Powers to Intercept Communications under National Security Law

A. Historical Development of the Foreign Intelligence Surveillance Act (FISA)

1. Initial version

The Foreign Intelligence Surveillance Act of 1978, 18 U.S.C. §§ 1801 et seq., was introduced as a bill on 18 May 1977 by Senator Ted Kennedy, and was signed into law in 1978 by then President Carter. The Act was the result of US Senate Committee investigations into President Richard Nixon's use of federal employees to spy on political groups.[139]

The FISA is the preeminent United States law regarding collection of "foreign intelligence information"[140] that is communicated or sent by "foreign powers"[141] or

---

[139] The leaders of the investigation were Senators Sam Irvin and Franck Church, which is why the Committee was sometimes referred to as the Church Committee. This committee, which was formally the United States Senate Committee to Study Governmental Operations with Respect to Intelligence Activities, ultimately became the US Senate Select Committee on Intelligence. In 1975 and 1976 the Church Committee published fourteen different reports regarding the intelligence agencies, their transgressions, and suggested reforms. These activities were well documented.

[140] Under 18 U.S.C. § 1801(e), foreign intelligence information means:

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

[141] Under 18 U.S.C. § 1801(a), foreign power is defined as follows:

(1) a foreign government or any component thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

"agents of foreign powers."[142] It sets forth specific standards that must be met in order to obtain evidence via wiretapping, physical searches, pen registers, trap and trace and other methods, which overlap with the methods authorized under the ECPA.[143] The Act contains limits on how these powers can be applied to "U.S.

---

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction."

[142] Under 18 U.S.C. § 1801(b), an agent of a foreign power is defined as follows:

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore;

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C)."

[143] See Liu, Edward C. *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services (April 8, 2013). Legislative attorney Edward C. Liu has a good discussion of the powers granted by the Electronic Communications Privacy Act as opposed to FISA: "ECPA provides three sets of general prohibitions accompanied by judicially supervised exceptions to facilitate law enforcement investigations. The prohibitions address (1) the interception of wire, oral, or electronic communications (wiretapping); (2) access to the content of stored electronic communications and to communications transaction records; and (3) the use of trap and trace devices and pen registers (essentially in-and-out secret "caller id" devices). In some circumstances, the use of surveillance activities for foreign intelligence purposes might fall within the scope of the activities prohibited by ECPA. There are two exceptions to ECPA's general prohibitions that address this situation. First, if the activity in question falls within the definition of electronic sur-

Persons." While more specifically defined in 18 U.S.C. § 1801, it refers to US citizens, lawfully admitted permanent resident aliens, and corporations incorporated within the United States.[144] It contains several sections that not only detail the procedure for applying for authorization for a warrant to seek certain foreign intelligence information, but also designates safeguards for violations thereof. The effectiveness of those safeguards has been called into question due to the secrecy of the FISA Court, and the fact that no one, as far as can be determined, has ever been sanctioned under those subsections. These procedures will nonetheless be discussed below.

2. The Patriot Act changes to the FISA

The USA Patriot Act of 2001 was signed into law on 26 October 2001, by then President George W. Bush. It was comprised of several bills that had not passed

---

veillance under FISA, then it may be conducted if the government complies with FISA's procedures. For example, the interception of a domestic telephone call is the type of activity that would generally be prohibited by ECPA. It would also qualify as electronic surveillance under FISA. Therefore, if the government obtained a court order from the FISC authorizing the interception of that call, it would be a lawful surveillance activity notwithstanding the general prohibition against wiretapping found in ECPA. Second, if the activity in question is not electronic surveillance, as that term is defined in FISA, but involves the acquisition of foreign intelligence information from international or foreign communications, then it is not subject to ECPA. For example, the interception of an international telephone call would not be considered electronic surveillance for purposes of FISA if the target were the person on the non-domestic end of the conversation and the acquisition would not occur on United States soil. So long as the purpose of that acquisition was to acquire foreign intelligence information, then it would not be subject to the general prohibitions in ECPA. Although both exceptions result in the non-application of ECPA, they differ in one important aspect that is particularly relevant to understanding the changes wrought by Title VII of FISA. Both ECPA and FISA provide that the two statutes constitute the exclusive means of conducting electronic surveillance, as defined in FISA. As a result, using the procedures under FISA is compulsory for those activities that qualify as electronic surveillance but cannot be accomplished by, and are exempt from, ECPA. In contrast, prior to the FISA Amendments Act, FISA's procedures were generally never needed for wiretapping activities that did not qualify as electronic surveillance, and which were also exempt from ECPA because they involved international or foreign communications. However, as discussed below, the recently added § 704 of FISA does make FISA's procedures compulsory when the target of such surveillance is a United States person. Those activities that remain beyond the scope of either ECPA or FISA are governed by Executive Order 12333 and the Fourth Amendment, discussed in the next two sections." See Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services, at 2-3 (8 April 2013).

144 Under 18 U.S.C. § 1801(i), the FISA defines United States person as "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section."

previously, cumulatively amending the Foreign Intelligence Surveillance Act of 1978, the Electronic Communications Privacy Act of 1986, as well as others. Consideration was short, as the country reeled from the 9/11 attacks. While the Patriot Act contained several controversial provisions, the most enduringly controversial ones were in Title II.

Title II amended the enhanced surveillance procedures. It allowed the government to collect information from both US citizens and non-US citizens. It then changed the FISA by no longer requiring that the gathering of foreign intelligence information be the primary purpose of a surveillance measure; it was henceforth sufficient that it was a "significant purpose."[145] This was done to remove the previous wall between foreign intelligence gathering and criminal investigations, since prior to the amendment, in order to use the powers set forth under FISA, the government had to show that the "primary purpose" was only to gather foreign intelligence information.

Title II also expanded criminal law enforcement powers by allowing: roving wiretaps, wiretapping of "protected computers" by consent, sneak and peak warrants, and greater powers for obtaining information from internet service providers via subpoena. Because these were controversial, however, the numerous sections were set to expire automatically on 31 December 2005, unless reauthorized.[146]

Title V contained another controversial provision. Under that section, National Security Letters were now able to be approved by the Special Agent in Charge of the FBI field office, whereas they used to require approval by the Deputy Assistant Director of the FBI.[147]

3. Protect America Act of 2007

In 2005, the New York Times issued a report that the US federal government had been monitoring international phone calls and emails without having obtained any kind of warrant.[148] Several parties have alleged that this was a sea-change in domestic surveillance, since the NSA traditionally had only performed surveillance outside the borders of the United States. President George W. Bush admitted that after the attacks of 11 September 2001, he authorized the NSA to execute a terrorist surveillance program, which allowed the NSA to conduct warrantless wiretaps of

---

[145] USA PATRIOT ACT (U.S. H.R. 312, Public Law 107-56), Title II, Sec. 218.

[146] Sections 201, 202, 203(b), 204, 206, 207, 209, 212, 214, 215, 217, 218, 220, 223, 225.

[147] USA PATRIOT ACT (U.S. H.R. 3162, Public Law 107-56).

[148] See Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services (April 8, 2013), citing, James Risen and Eric Lichtblau, Bush Lets US Spy on Callers Without Courts, N.Y. Times, 16 December 2005, at 1.

communications into and out of the United States if, essentially, they were linked to terrorist organizations.[149] The administration had asserted, however, that the Authorization for Use of Military Force,[150] passed by Congress on 14 September 2001, along with the President's inherent authority under Article II of the United States Constitution superseded the warrant requirements of the FISA. This seemingly continued until January of 2007.[151] Due to uncertainty on that position, on 28 July 2007, then President Bush announced he had submitted a bill to amend the FISA. It was passed by Congress on 3 August 2007.

The bill altered the FISA in several ways. First and foremost, it redefined "electronic surveillance" so that such term would not be "construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States."[152] It also changed the warrant and notification requirements. It eliminated the need for a warrant, instead substituting several areas of internal controls. It did require notification to the FISA court if any warrantless surveillance had been conducted within 72 hours of said surveillance. The amendments made clear that a person on a phone in the United States talking with someone from outside the US could be wiretapped, so long as the person within the US was not a target of the investigation. It did install reporting requirements to Congress, though they were quite minimal. They included reporting on: 1. incidents of corporation non-cooperation, 2. incidents of non-cooperation, 3. the number of certifications and directives, and 4. reports of procedural failures. These powers were temporary and expired on 16 February 2008.[153]

4. FISA Amendments Act of 2008

On 10 July 2008, George W. Bush signed the FISA Amendments Act (FAA) into law.[154] It performed several functions. First, new sections to the FISA almost identical to the old FISA were added, in the form of a new Title VII, which was very similar to the provisions of the Protect America Act of 2007, which expired earlier in 2008. Under the FAA, the "Attorney General and the DNI may authorize jointly,

---

[149] See Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services, at 4 (8 April 2013).

[150] Pub. L. 107-40.

[151] See Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services, at 5 (8 April 2013), citing, S. Rept. 110-209, at 4. See also Letter from Attorney General Gonzales to Senate Judiciary Committee Chairman Patrick Leahy and Senator Arlen Specter (17 January 2007).

[152] See 50 U.S.C. § 1801.

[153] See Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, p. 2, Congressional Research Services at 5 (8 April 2013).

[154] FISA Amendments Act of 2008, Pub. L. No. 110-261, § 403, 122 Stat. 2463, 2473 (2008).

for up to one year, the 'targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.'"[155]

These procedures affected both US persons and non-US persons, specifically adding:

– a new procedure for targeting non-U.S. persons abroad without individualized court orders;[156]

– a new requirement to obtain an individualized court order when targeting U.S. persons abroad;[157] and

– new procedures that can be used to obtain court orders authorizing the targeting of U.S. persons abroad for electronic surveillance, the acquisition of stored communications, and other means of acquiring foreign intelligence information.[158]

These procedures are, of course, contained in one of a few federal laws that allows for the use of electronic surveillance.

5. Extensions of amendments in 2011

On 26 May 2011, President Obama extended three amendments to FISA to 1 June 2015. Those Amendments were originally passed as part of the USA Patriot Act,[159] in the wake of the attacks of 11 September 2001. Recognizing that at least three of the powers granted thereby were controversial, the United States Congress established sunset provisions. These powers include:

– Section 6001(a) of the Intelligence Reform and Terrorism Prevention Act (IRTPA), also known as the "lone wolf" provision, which simplifies the evidentiary showing needed to obtain a FISA court order to target non-U.S. persons who engage in international terrorism or activities in preparation therefore, specifically by authorizing such orders in the absence of a proven link between a targeted individual and a foreign power;

– Section 206 of the USA PATRIOT Act, which permits multipoint, or "roving," wiretaps (i.e., wiretaps which may follow a target even when he or she changes phones) by adding flexibility to the manner in which the subject of a FISA court order is specified; and

– Section 215 of the USA PATRIOT Act, which broadens the types of records and other tangible things that can be made accessible to the government under FISA.[160]

The sunset provisions require those parts of the USA Patriot Act to be reapproved annually.

---

[155] Blum, Stepanie Cooper, *What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 Pubic Interest Law Journal 269, 297.

[156] Citing 50 U.S.C. § 1881a.

[157] Citing 50 U.S.C. § 1881c(a)(2).

[158] Citing 50 U.S.C. §§ 1881b, 1881c. See Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, p. 2, Congressional Research Services (8 April 2013).

[159] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, P.L. 107-56 (2001).

[160] Liu, Edward C., *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, CRS Report R40138 (16 June 2011).

6. Renewal of FISA Amendments Act

On 30 December 2012, President Obama signed into law H.R. 5949, otherwise known as the Foreign Intelligence Surveillance Act Amendments Reauthorization Act of 2012. This extended Title VII of FISA until 31 December 2017. Title VII of FISA had been added by the FISA Amendment Act of 2008. It created a new procedure for targeting non-US persons, as well as US persons reasonably believed to be outside of the United States.[161] This was immediately challenged by several lawsuits.

In February of 2013, however, the United States Supreme Court passed judgment on the constitutionality of the Foreign Intelligence Surveillance Act Amendments Reauthorization Act of 2012. In *Clapper v. Amnesty International*, the US Supreme Court dismissed the suit on the basis that none of the plaintiffs had suffered enough definite injury to have standing to challenge Title VII.[162]

B. Summary of Current Abilities to Collect Foreign and National Intelligence Information

1. Executive Order 12333

One of the other two ways to legally authorize electronic surveillance is under Executive Order 12333. This Executive Order states in section 2.5, as amended, that the Attorney General has the power to approve the use of any technique for intelligence purposes against a US person abroad, or anywhere within the United States.[163] However, if a warrant would otherwise be required, the Attorney General must make the additional determination that the technique being utilized is directed against either a foreign power or an agent thereof.[164] This authority must comply with FISA, but also goes beyond the powers granted to the Attorney General by FISA.[165]

2. FISA authorizations

Different sections of Title 50 deal with different aspects of collection of data. Subchapter I covers electronic surveillance, generally, and is composed of Sections 1801–1812. The FISA provides a procedure for the President of the United States

---

[161] See Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services (8 April 2013).

[162] See *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013).

[163] See Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services at 3 (8 April 2013).

[164] Id.

[165] Id.

to order electronic surveillance without a court order under certain limited circumstances.[166] Therein, such procedure is legal if the Attorney General certifies in writing and under oath that the electronic surveillance meets the following three criteria:

(A) the electronic surveillance is solely directed at

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801 (a)(1), (2), or (3) of this title; or

(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801 (a)(1), (2), or (3) of this title;

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801 (h) of this title.

The minimization procedures[167] are defined in Section 1801(h), and contain four provisions. The first is that the Attorney General shall adopt such procedures "reasonably designed" to minimize the "acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning nonconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[168] The second requirement prohibits dissemination of the identity of any non-consenting United States person "unless such person's identity is necessary to understand foreign intelligence information or assess its importance."[169] Third, it must include procedures that permit

---

[166] See 18 U.S.C. § 1801(a)(1).

[167] The term minimization procedures are defined under 18 U.S.C. § 1801(h) 1-4 as follows:

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802 (a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

[168] See 18 U.S.C. § 1801(h)(1).

[169] See 18 U.S.C. § 1801(h)(2).

the "retention and dissemination" of "evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes."[170] The fourth requirement for minimization procedures requires that "no contents of any communication to which a United States person is a party" may be "disclosed, disseminated, or used for any purpose or retained for longer than 72 hours" unless a court order under section 1805 is obtained, or if the Attorney General has decided that "the information indicates a threat of death or serious bodily harm to any person."

Subchapter II governs physical searches and is made up of Sections 1821–1829. Subchapter III deals with pen registers and trap and trace devices for foreign intelligence purposes (Sections 1841–1846). Subchapter IV deals with access to certain business records for foreign intelligence purposes (Sections 1861–1863). Subchapter V specifies the reporting requirements and only contains Section 1871. Subchapter VI covers additional procedures regarding persons outside of the United States (Section 1881). Lastly, Subchapter VII provides protections for those persons assisting the government (Section 1885).

3. Surveillance of persons physically outside of the United States

Section 1881a provides for electronic surveillance of persons outside of the United States: "[t]he Attorney General and Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[171] Subsection b, however, then immediately lays out the limitations, in that the actions authorized under subsection (a):

> (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
>
> (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
>
> (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
>
> (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
>
> (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.[172]

There is a requirement for the joint authorization of the Attorney General and Director of National Intelligence. Such authorization must be based upon either the

---

[170] See 18 U.S.C. § 1801(h)(3).

[171] 50 U.S.C. § 1881a(a).

[172] 50 U.S.C. §1881a(b).

existence of a court order approving a joint certification submitted by the AG and DNI, or a determination by the two officials that exigent circumstances exist."[173]

Any such acquisition must be accomplished in accordance with both the targeting and the minimization procedures established by the Attorney General and the Director of National Intelligence. It also requires submission of a certification.[174] And just in case anyone believed that a warrant might still be required, subparagraph 4 explicitly dispels that notion: "[n]othing in subchapter I shall be construed to require an application for a court order under such subchapter for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States."[175]

Pursuant to this subchapter, the Attorney General and the Director of National Intelligence may directly order electronic communication service providers to:

(A) immediately provide the government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

Of course, the providers get something for this cooperation. They get compensated at the prevailing rate: "for providing information, facilities, or assistance."[176] They also get a complete release from being sued by anyone for providing such assistance.[177]

Even though a judge does not oversee the issuance of the directive, there are procedures for challenging it. An electronic communication service (ECS) provider receiving such a directive may file a petition to modify or set aside such directive. That petition, however, is filed directly with the Foreign Intelligence Surveillance Court (FISC). The original directive stands unless the presiding judge of the FISC determines that the directive at issue doesn't meet the requirements of this section "or is otherwise unlawful." The judge can also ask for a plenary review by the whole court. Either the government or the ECS provider subject to the directive could then file a petition with the Foreign Intelligence Surveillance Court of Review (FISCR) for a review of such decision rendered under subsections 4 or 5. The

---

[173] See Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services at 6 (8 April 2013).

[174] See 50 U.S.C. § 1881a(c).

[175] See 50 U.S.C. § 1881a(c)(4).

[176] See 50 U.S.C. § 1881a(h)(2).

[177] See 50 U.S.C. § 1881a(h)(3).

FISCR then must provide a written "statement for the record of the reasons for such determination."[178] If the ECS provider doesn't comply, however, "the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition."[179] The presiding judge must assign a judge to the petition within 24 hours and then that judge must issue an order within thirty days.[180] Subsection (i) provides for review of certifications and procedures, with a very similar mechanism to that described above for directives.[181]

4. Notifications

The whole process remains secret from the general public. Under 50 U.S.C. § 1881a(k), the FISC shall maintain records of these proceedings. However, "[a]ll petitions under this section shall be filed under seal."[182] Nevertheless, the "Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued."[183]

There is a review procedure for assessment of the program. Not less than every 6 months, the Attorney General and Director of National Intelligence "shall assess compliance with the targeting and minimization procedures" and shall submit their report to:

(A) the Foreign Intelligence Surveillance Court; and

(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution

(i) the congressional intelligence committees; and

(ii) the Committees on the Judiciary of the House of Representatives and the Senate.[184]

These reports then go to the Attorney General, the Director of National Intelligence and the congressional committees referred to above as part of the semi-annual review procedure. Indeed, even further review is mandated. There must be an annual review conducted by the head of each element of the intelligence community conducting electronic surveillance under this section. The review shall provide:

---

178 See 50 U.S.C. § 1881a(h)(4)(D).

179 See 50 U.S.C. § 1881a(h)(5).

180 See 50 U.S.C. § 1881a(h)(5).

181 See 50 U.S.C. § 1881a(i).

182 See 50 U.S.C. § 1881a(k).

183 See 50 U.S.C. § 1881a(k)(3).

184 50 U.S.C. § 1881a(m).

(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;

(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.[185]

Those heads must then use these procedures to determine the adequacy of the aforesaid minimization procedures and how they were used.[186] In turn, those reviews must be provided to the FISC, the Attorney General and the congressional committees referred to above.[187]

IV. Information Sharing

A. Domestic Exchange of Information

It has long been a fundamental principle of US law that information collected under the powers to keep the United States secure[188] is completely separate from

---

[185] 50 U.S.C. § 1881a(m)(3).

[186] See 50 U.S.C. § 1881a(m)(3).

[187] See 50 U.S.C. § 1881a(m)(3).

[188] The intelligence community includes:

"(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

(11) The Office of Intelligence and Counterintelligence of the Department of Energy;

(12) The Bureau of Intelligence and Research of the Department of State;

(13) The Office of Intelligence and Analysis of the Department of the Treasury;

the information collected to protect the safety of America through enforcement of its criminal laws. There are numerous safeguards in place to protect civil liberties in the prosecution of criminal acts.[189]

There is a long history of the legal precedent used to collect information under national security law. However, this article shall only go back about 18 years in this respect. On 11 September 2001, the US intelligence community failed to prevent attacks in New York, Washington, DC, and Pennsylvania committed by terrorists hijacking airplanes and flying them into targets. This was viewed as a significant failure of the US intelligence system and caused a major report to be produced to determine what, if anything, could have been done differently to prevent it. The result was the Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of 11 September 2001.[190] That committee made the finding:

> "Within the Intelligence Community, agencies did not adequately share relevant counterterrorism information, prior to September 11. This breakdown in communications was the result of a number of factors, including differences in the agencies' missions, legal authorities and cultures. Information was not sufficiently shared, not only between different Intelligence Community agencies, but also within individual agencies, and between the intelligence and law enforcement agencies."[191]

This supported the changes that were made in the USA Patriot Act, which were a major change to prior policy of keeping those efforts "walled off from one another through a complex arrangement of constitutional principles, statutes, policies and practices."[192] Prior to the USA Patriot Act, there had been several efforts to regu-

---

(14) The Office of Intelligence and Analysis of the Department of Homeland Security;

(15) The intelligence and counterintelligence elements of the Coast Guard; and

(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community." See Executive Order 12333, United States Intelligence Activities, as amended by Executive Orders 132 (2003), 13355 (2004) and 13470 (2008), paragraph 3.5(h).

[189] See Schwerha, Kaspersen, and Dragicevic, *Article 15 Conditions and Safeguards under the Budapest Convention on Cybercrime*, Cybercrime@IPA, EU/COE Joint Project on Regional Cooperation Against Cybercrime, 29 March, 2012.

[190] U.S. Congress, 107th Congress, Senate, Select Committee on Intelligence, and House of Representatives, Permanent Select Committee on Intelligence, Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attack of September 11, 2001, Report, S.Rept. 107-351, H.Rept. 107-792, December 2002, p. 33.

[191] Id. at p. xvii.

[192] Best, Richard A. Jr., *Sharing Law Enforcement and Intelligence Information: The Congressional Role*, CRS Report for Congress, Congressional Research Service, RL33873 (13 February 2007). Traditionally, intelligence agencies concentrate on efforts outside of US territory, including the National Security Agency, the Central Intelligence Agency, the National Reconnaissance Office, the National Geospatial-Intelligence Agency, the Department of Homeland Security, the Bureau of Intelligence and Research of the State Department, as well as intelligence components of the military.

late this type of information sharing.[193] On 26 October 2001, the Patriot Act was made law, significantly changing the information sharing landscape.

In this regard, the Patriot Act made several changes. A discussion of all of the changes is beyond the scope of this chapter. However, some of the most significant changes for the purposes of our subject were:

1. It changed the requirement that FISA surveillance had to have a primary purpose of collecting foreign intelligence information to the new requirement that the collection of such information only had to be "a significant purpose" of collecting foreign intelligence information. Afterwards, FISA authority could be used to collect information where criminal investigation was the primary purpose.[194]

2. Section 504 explicitly now allowed federal officers conducting electronic surveillance and physical searches under FISA to consult with law enforcement officers at the federal, state, and local levels under certain circumstances relating to attacks, sabotage, international terrorism or attempts to collect intelligence by foreign powers.[195]

Likewise, the Patriot Act was followed by the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act 2004, which also created new procedures for sharing intelligence information about international terrorism. The latter also created the Information Sharing Environment (ISE), which was later supplemented by an implementation plan issued by the administration.[196, 197]

Because of the numerous safeguards in effect for interception of telecommunications for law enforcement purposes, there are few restraints, if any, for information obtained thereby being shared with the national security community, aside from those set forth in the general law on that matter. However, because there are fewer civil rights protections in place for acquisition of such information for national security purposes, the sharing of information legally obtained for national security purposes with law enforcement is more closely regulated. While a complete review of policy and law is beyond the scope of this chapter, one may primarily look to 50 U.S.C. § 1806(b), Executive Order No. 12333 and, where applicable, the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes" or any successor document.

50 U.S.C. § 1806 is entitled "Use of Information" under the Electronic Surveillance chapter. It provides that such information may be shared only pursuant to the

---

193 See Sharing Law Enforcement and Intelligence Information, infra, at pp. 6–10.

194 Id. p. 11.

195 Id. at pp. 11–13.

196 Id. at 14.

197 Reuters, Exclusive: U.*S. Directs Agents to Cover Up Program Used to Investigate Americans*, 6 August 2013, available 7 August 2013 at http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805

minimization procedures required by that subchapter, that such information does not automatically lose its privileged character and that any sharing must only be for a lawful purpose.[198] Section 1806 also then provides restrictions on the use of the information, including notification to the targets of the intended use of the information and opportunities to challenge its use.[199]

B. Exchange of Intercepted Electronic Communications Data between Foreign Countries

Traditionally, the United States has exchanged intercepted data via letters rogatory, requests under Mutual Legal Assistance Treaties (MLATs), and perhaps even informal requests. While the statistics regarding the frequency of same are hard to assess, it would appear that requests under MLATs have been the most common, at least until recent times. As has been recently stated:

> "[s]tatistical information about MLATs, such as the number of requests filed by various countries or how long a request usually takes, is often difficult or impossible to locate. [5] DOJ's budget request for FY 2016 indicates that in 2000, the United States sent over 500 MLA requests and received over 1,500. [6] Since then, the numbers have steadily grown; the recent budget request indicates that in 2014, the United States sent over 1,000 requests and received around 3,250. [7] It further reflects that OIA had over 4,800 pending requests in 2014, even after instituting an internal policy for 'refusing cases on de minimus grounds.' [8] But there is little other information regarding MLAT requests made available to the public."[200]

However, with the passage of a major piece of legislation, the landscape has changed.

The Clarifying Lawful Overseas Use of Data (CLOUD) Act[201] has two major facets: the US government's ability to compel technology companies to disclose the contents of electronic communications stored on the companies' servers and data centers overseas, and the reciprocal issue of foreign governments' ability to access data in the United States. It is one of the first major changes in years to US law governing cross-border access to electronic communications held by private companies. The CLOUD Act responds to calls for modernization by authorizing the executive branch to conclude a new form of international agreement through

---

198 50 U.S.C. § 1806(a).

199 50 U.S.C. § 1806(b).

200 See Lifting the Veil on the MLAT Process: A Guide to Understanding and Responding to MLA Requests, K&L Gates Hub, January 20, 2017 (accessed 6 August 2020 https://www.klgates.com/lifting-the-veil-on-the-mlat-process-a-guide-to-understanding-and-responding-to-mla-requests-01-20-2017/).

201 H.R. 4943 (Pub. L. 115-141) was passed with the passing of the Consolidated Appropriations Act, 2018, PL 115-141, Division V., which was the Omnibus Budget Bill that was signed by President Trump on 23 March 2018.

which select foreign governments can seek data directly from US technology companies without individualized review by the US government.

The CLOUD Act is a legislative response to the legal question raised in *United States v. Microsoft* under the Stored Communications Act (SCA), which is part of the broader Electronic Communications Privacy Act (ECPA).[202] At that time, there were two common international legal processes for obtaining a warrant required for electronic communication disclosure: letters rogatory requests and MLATs. The CLOUD Act will supplement, not replace, these existing avenues of international data sharing.[203]

The CLOUD Act creates a third paradigm of international data sharing arrangements: the possibility of international agreements that remove legal restrictions on US technology companies' ability to disclose data directly to certain foreign nations in response to "orders" issued by foreign nations.[204] The CLOUD Act authorizes the United States to enter "executive agreements" with qualifying foreign nations,[205] unlike MLATs, which are "treaties," and letters rogatory, which are court to court requests. The executive agreements authorized under the CLOUD Act would allow service providers to disclose the contents of electronic communications– both stored communications and real-time communications intercepted by wiretap – directly to requesting foreign governments with whom the United States has an authorized data sharing agreement.[206]

United States v. Microsoft arose out of the issue of extraterritorial application of the SCA.[207] Federal law enforcement officials sought an SCA warrant requiring Microsoft to disclose all emails and other information associated with an account with one of its customers.[208] However, some of the user's data was stored on a server in Ireland.[209] Microsoft declined to comply with the portion of the warrant seeking data stored overseas on the ground that the SCA's mandatory disclosure provisions did not apply extraterritorially.[210] The US Court of Appeals for the Second Circuit (Second Circuit) then held that the SCA does not authorize the seizure of emails stored exclusively on foreign servers.[211]

---

202 See 18 U.S.C. § 2702(a)(3).

203 See CLOUD Act § 106.

204 See id.

205 CLOUD Act § 105.

206 See CLOUD Act § 104.

207 See *United States v. Microsoft* Corp., No. 17-2, 548 U.S. __, 2018 WL 1800369, slip op. at 2 (U.S. Apr. 17, 2018) (per curiam).

208 See id. at 1.

209 *Matter of Warrant*, 829 F.3d 197, 204 (2nd Cir. 2016).

210 Id. at 205.

211 See id. at 222.

While the *Microsoft* appeal was pending before the Supreme Court, officials from the Department of Justice (DOJ) sought a legislative response to the Second Circuit's ruling.[212] The DOJ argued that the Second Circuit's decision "effectively hamstrung the ability of law enforcement" to obtain data stored by US service providers abroad, creating a "tremendous problem" that caused "substantial harm to public safety."[213]

As enacted, the CLOUD Act amends ECPA by, among other things, including the following extraterritoriality provision:

> A [provider] shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.[214]

After the CLOUD Act's enactment, the Supreme Court concluded that the case had become moot, and vacated the lower court's rulings with instructions to dismiss.[215]

Besides its addition of the extraterritoriality provision, the CLOUD Act also contains provisions designed to resolve potential conflicts of law that could arise if the United States seeks data stored abroad when the law of a foreign country prohibits disclosure.[216] It does so by authorizing a provider to file a motion to quash or modify a data demand if:

1. the provider reasonably believes the target of the demand is not a US person and does not reside in the United States;
2. the provider reasonably believes disclosure would create a material risk of violating a foreign nation's law; and
3. the foreign nation whose law may be violated has a data sharing agreement with the United States authorized by the CLOUD Act.[217]

A court may grant the providers' motion to modify or quash a government demand for data upon finding that three conditions are met:

1. the required disclosure would violate foreign law;

---

[212] Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary, 115th Cong. 1 (2017) [hereinafter Data Stored Abroad Hearing].

[213] Data Stored Abroad Hearing (statement of Richard W. Downing, Acting Deputy Assistant Att'y Gen., U.S. Dep't of Justice), https://judiciary.house.gov/wp-content/uploads/2017/06/DowningTestimony.pdf

[214] CLOUD Act § 103(a)(1) (adding 18 U.S.C. § 2713).

[215] *United States v. Microsoft* Corp., No. 17-2, 548 U.S. __, 2018 WL 1800369, slip op. at 2 (U.S. 17 April 2018).

[216] CLOUD Act § 103(b) (adding 18 U.S.C. § 2703(h)).

[217] Id.

2. the interests of justice dictate that the demand should be quashed or changed; and
3. the target is not a US person and does not reside in the United States.[218]

The CLOUD Act does not specify by name which countries meet its requirements. Instead, it contains requirements for the governments with whom the United States can enter agreements and the nature of demands foreign governments can make.[219] Before an agreement concluded under the CLOUD Act can enter into force, the Attorney General, with the agreement of the Secretary of State, must make four written certifications that are provided to Congress and published in the Federal Register:

1. the foreign nation's domestic law "affords robust substantive and procedural protections for privacy and civil liberties" in its data-collection activities, as determined based on at least seven statutory factors;
2. the foreign government has adopted "appropriate" procedures to minimize the acquisition, retention, and dissemination of information concerning US persons;
3. the executive agreement will not create an obligation that providers be capable of decrypting data, nor will it create a limitation that prevents providers from decryption; and
4. the executive agreement will require that any order issued under its terms will be subject to an additional set of procedural and substantive requirements.[220]

The fourth certification required by the CLOUD Act mandates that any data sharing agreement concluded under the Act contains a set of requirements relating to foreign governments' orders issued to service providers. These include, among other things, requirements that all orders identify a specific person, account, or other identifier that is the object of the order:

1. be premised on a "reasonable justification based on articulable and credible facts, particularity, and severity regarding the conduct under investigation;"
2. not intentionally target a US person (or person located in the US) or target a non-US person with the intention of obtaining information about a US person;
3. be issued for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of a "serious "crime"—a term that the CLOUD Act states includes terrorism, but otherwise does not define;
4. comply with the domestic law of the issuing country;
5. not be used to infringe freedom of speech; and
6. satisfy additional requirements for real-time communications captured by wiretap.[221]

---

[218] Id.

[219] See id.

[220] See CLOUD Act § 105 (adding 18 U.S.C. § 1253).

The CLOUD Act has the potential to result in a three-tiered system for cross-border data sharing in criminal matters. Those nations that are approved for CLOUD Act agreements could request data directly from US service providers in cases involving "serious crimes" – provided they do not target US persons or persons located in the United States and meet the CLOUD Act's other requirements. For nations that have an MLAT but no CLOUD Act agreement, or for data requests that fall outside the scope of the CLOUD Act, foreign governments can use the MLAT process. Finally, private litigants and nations that do not have a CLOUD Act agreement or an MLAT may request that their courts issue letters rogatory to the courts of the United States.

While the CLOUD Act is likely to more clearly define the scope of US officials' right to seek certain data stored overseas in the custody of US providers, its broader impact on the international data sharing regime is less certain. As the internet continues to expand and become more globalized, law enforcement officials worldwide can be expected to continue to seek access to data stored on servers outside their territorial jurisdictions. Many nations could pursue CLOUD Act agreements, which would provide faster access to data held by US providers. Whether the United States ultimately enters such agreements will depend on the willingness of the executive branch to certify foreign nations' eligibility and Congress's desire to block a proposed agreement through a joint resolution of disapproval enacted into law.

The impact of the CLOUD Act on privacy, human rights, and civil liberties interests similarly is difficult to predict. The Act has the potential to create a three-tiered system of international data sharing, with the United States' most trusted foreign partners able to obtain data directly from US companies without individualized review by the US government. Because this system of direct access differs from existing international data sharing regimes, the manner in which data requests are administered, the type of data that is collected, and the degree of potential for abuse of the system, if any, may become more apparent over time.

---

[221] See CLOUD Act § 105 (adding 18 U.S.C. § 1253).

List of Abbreviations

AG	United States Attorney General
CALEA	Communication Assistance for Law Enforcement Act
CLOUD Act	The Clarifying Lawful Overseas Use of Data Act
Cong. Research Serv.	Congressional Research Service
CRS	Congressional Research Service
DA	District Attorney
DC	District of Columbia
DEA	United States Drug Enforcement Agency
DNI	United States Director of National Intelligence
DOJ	United States Department of Justice
ECPA	Electronic Communications Privacy Act of 1986
ECS	electronic communications service
EFF	Electronic Frontier Foundation
FBI	United States Federal Bureau of Investigation
FCC	United States Federal Communications Commission
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court of Review
ISE	Information Sharing Environment
MLAT	mutual legal assistance treaty
NSA	United States National Security Agency
P.L.	Public Law
SCA	Stored Communications Act
US	United States
USA	United States of America
U.S.C.	United States Code
U.S.C.A.	United States Code Annotated
USA Patriot Act of 2001	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism of 2001
VoIP	Voice over internet protocol

Appendix: Questionnaires

Ulrich Sieber
Nicolas von zur Mühlen
Max Planck Institute for Foreign and International Criminal Law

Contents

Max Planck Institute for Foreign
and International Criminal Law
79100 Freiburg i.Br. / Germany
– Department for Criminal Law –
Prof. Dr. Dr. h.c. mult. Ulrich Sieber

International Legal Cooperation in the Interception of Telecommunication

– Guide for the Interviews with Representatives of LEAs and Government –

(INTLI-Research Doc. No. 2 – V 2.0)

Function of this Document

The INTLI-study of the Max Planck Institute for Foreign and International Criminal Law in Freiburg/Germany aims to improve mutual legal assistance for the interception of telecommunication (INTternational Legal Interception – INTLI). Special focus lies on the question, whether and how intercepted data can be exchanged in real time between different national (esp. European) criminal justice systems, thus making investigation and prosecution of serious crimes more effective without undue limitations of the civil liberties of citizens. The structure of the expected general report will be specified in accordance with the progress of the study in INTLI-Doc. No. 1.

The research is based on a study of the respective national laws and the relevant international instruments ("law in the books") and on the present practices in the various national criminal justice systems ("law in action"). This twofold approach is reflected in two questionnaires that focus on legal and practical aspects of lawful interception, and, thus, complement each other: **The practice of the law in action is investigated by interviews with practitioners (esp. from LEAs and Government) in the field of telecommunication interception; these interviews are structured and harmonized by the on hand interview guide draft INTLI-Doc. No. 2.** The law in the books is analyzed by country reports on the national legal situation following a common structure and common questions described in draft INTLI-Doc. No. 3.

Contents of INTLI Doc No. 2

Guide for the Interviews with Representatives of LEAs and Government

Guide for the Interviews with Representatives of LEAs and Government

I. General Information

1. [Acknowledgement for the invitation and the willingness to cooperate. Short presentation of the interviewer, the Max-Planck Institute for Foreign and International Criminal Law Freiburg, its experience with practice-oriented studies, its cooperation with German investigative authorities in the present project. Explanation of the aims and methods of the project.]

2. [Introductory questions for the interviewed person(s): esp.:] What is your professional background and your present task? For how many years have you worked in the field of telecommunication interception and related fields? How many national and international interception procedures have you been involved in personally?

II. National Procedures

3. Which institutions deal with electronic interception in your country and what are the respective procedures in criminal matters? What is the relationship of telecommunication surveillance in criminal matters with interception procedures in preventive police activities, and with intelligence services and other institutions?
   Express note: All following questions will deal only with interception in *criminal* matters (criminal procedural law).

4. For which types of crimes (or dangers) is interception primarily used in practice? How important is electronic interception of content data for investigating crimes in your country? Can you compare the importance of analyzing content data with the importance of analyzing meta data (traffic data) for criminal investigations?

5. What is the procedure for interception in criminal justice matters in your country? Are there emergency procedures (e.g. not requiring a court order)?

6. Are there restrictions on the interception of telecommunications of specific persons (e.g. privileges for medical doctors, attorneys, journalists, priests)? To which extent do these privileges also apply if the said person is suspected of a serious crime? Do you also have a restriction on intercepting or analyzing data concerning the core area of privacy (e.g. communication on sexual activities, prayer).

7. How is the individual interception of electronic communication technically handled in your country?

a) Are there centralized institutions (e.g. for the whole country) or different types of institutions?

b) Is interception only executed through orders of state institutions given to service providers or also by state authorities acting on their own (e.g. by using IMSI-catchers or intercepting satellite communications)?

8. Most countries differentiate in their criminal procedural codes between criminal procedural provisions on telecommunication interception and / or provisions on search and seizure.

a) Which of these provisions and which procedures (if any) are used in your country to access emails stored on a mail provider and data stored on an online storage service (e.g. a user's cloud)?

b) Is there a difference if access to these data is attained by a single (possibly open) procedure or by permanent (clandestine) surveillance?

c) What is the legal basis in these cases?

9. Interception of IP traffic (e.g. from internet access points, DSL routers, internet nodes, cable nodes, LTE or UMTS nodes) captures not only communication between persons but – in the same data stream – also communication between users and automated computer systems (e.g. user's access to websites, communication between a user's computer and his cloud, or communication between automated systems (e.g. in the "internet of things" such as connected home products).

a) Do you usually intercept and collect *all* of these types of communication when you intercept IP-traffic?

b) Are there any legal problems in collecting all these types of data under an interception order of your legal system (e.g. because they are not considered a communication between two persons)? Could you e.g. get an interception order for intercepting and analyzing the websites which are visited by the suspect? Is this question already being discussed in your country and is there any jurisprudence on this topic?

c) Esp. if you are not entitled to intercept or use some types of these IP data: how, where, and by whom are these data filtered out of the general IP-data stream and separated from the traditional telephone or telecommunication data?

d) To what extent is it necessary to intercept and to collect all these types of communication between humans and machines (e.g. access of a user to visited websites) for an effective interception of electronic communication in order to capture possible communication between two persons who are using innovative information channels? What are you doing to capture hidden electronic communication using internet protocols and IP-ports that are not normally used for human communication?

10. For technical reasons interception of telecommunication data sometimes captures data which cannot be legally intercepted due to legal privileges protecting the professional secrecy of doctors, attorney, journalists, priests, etc. The same could apply if interception of data involves the core area of privacy (e.g. communication on sexual activities). How do you handle this problem of undue or excessive data collection including data which are not targeted for legal reasons? How, where, and by whom are data streams which possibly contain such undue data analyzed and filtered out?

11. Is it technically possible for investigative agencies of your country to access encrypted telecommunication by (clandestine) remote access to the computers of the communicating partners (so-called source telecommunication surveillance capturing specific communication data before encryption or after decryption) in the course of criminal investigations? Is this practiced? What is the legal basis for this procedure (e.g. traditional interception provision or a special provision)?

12. For criminal matters, do investigation agencies access or supervise in specific serious cases all other (general) data by covert remote access to the computers of suspects? If not: Could they do this under your criminal procedural law? What is the legal basis for this procedure? Is there a reform discussion on this issue in your country?

13. Which internet providers can be a subject of the judicial warrant to intercept communications, e.g. access providers on the IP-transport level, infrastructure providers working on the IP-transport level or providers working on the IP-application level providing social interaction (e.g. e-mail or phone services, social networks) or data storing/processing services (e.g. cloud-providers or IoT services)?

14. What are the main practical problems for intercepting electronic communication in your country? How does your country handle these practical problems (e.g. encrypted data, questions of retaining traffic data by the providers)? What should be changed (technically, organizationally or legally) for improving the situation?

15. Can data resulting from a legal interception of telecommunication in criminal matters be used in criminal (court) proceedings in general? In which cases of illegal interception is it not possible to use intercepted data (just give a short description, no details)?

16. Who controls the interception of electronic communication in criminal matters? Esp., how intensively are applications for an interception order scrutinized by a *judge* in practice and to which extent is the judge realistically able to verify the evidence submitted by the applicant? How much information/evidence do you need to submit in order to have your application approved? How often are applications rejected by the judge? Are there other independent bodies of oversight (other than a judge) and how do they function?

17. Did you have any court decisions limiting the interception of telecommunication on *constitutional* grounds?

18. Are there any specific concepts (best practices) for the interception of electronic communication in your country which are highly successful for investigations or which protect civil liberties in a very efficient way and which you would recommend to other countries?

19. In which laws and guidelines are the interception issues discussed in the present interview regulated? Is there a regulation or a technical protocol for the technical specificities of internet providers? Could we get copies or web-addresses of these national regulations (if possible in English, French, or German)?

20. Are there any reform discussions (legislative or other) with respect to the discussed interception questions? What are the motives?

III. International Cooperation

21. How important is *transnational* electronic interception in foreign countries for your criminal justice system? Would a greater or a lesser extent or speed of foreign communication interception have a significant impact on the efficiency of your criminal justice system? Esp. for which types of cases? Could you specify distinctions between cooperation among EU countries and cooperation with other foreign countries?

22. a) What is the procedure for **obtaining** electronic interception in a foreign country? How often are requests for **obtaining** foreign interception successful, how often are they refused, and how often are they not answered? What are the grounds for refusal or for not answering the requests? Are there specific (legal, technical, organizational) obstacles for obtaining electronic interception in foreign countries (or in a specific foreign country)? Are your foreign partners filtering specific sensitive data out of the collected traffic before they transmit them to you (e.g. data on professional secrets, data on national security, specific types of data)? How effectively does international cooperation in electronic interception work in practice?

    b) What is the parallel situation for **granting** electronic interception in favor of a foreign country? Esp.: What are the reasons for which you as requested authority deny, limit, or delay requests for interception from other countries? If a request for legal interception is generally granted and you send the intercepted data from your country to the foreign police or judicial authority, do you check these data beforehand (for which purpose and with respect to which criteria?) or can you send the data unfiltered and unchecked as they are recorded?

23. a) How long does it take to initiate a procedure **for obtaining** interception in a foreign country?
    If the MLA-procedure is successful and data are gathered in the requested country, how long does it take to receive the respective data after the communication has been intercepted?
    By which technical means (e.g. discs, internet) are the data transmitted between the national police organizations?
    Do you get direct (online) real-time access to interception equipment installed in the foreign country? If not, (why) is this (technically, organizationally, or legally) not possible or problematic?

24. b) What is the parallel situation for **granting** electronic interception in favor of a foreign country, esp. regarding the duration of procedures and real-time access? In case your country is **granting** electronic interception, do you store data that has been intercepted after it has been transferred (immediately or subsequently) to the requesting state (e.g. in case of parallel investigations, for sampling inspection, data protection purposes, for general purposes, …)?

25. a) How do you handle the problem of data *obtained* from a foreign country which fall under legal privileges in your country (e.g. due to client-attorney privileges)?

    b) How do you handle the problem of *transmitting* data to a foreign country which fall under legal privileges in your country?

26. a) Under some mutual cooperation agreements (e.g. EU-MLA-requests for electronic interception), a *requested state* (who is asked to provide data for MLA) can make his consent subject to any condition which would have to be observed in a similar national case. Do you know about such demands? What demands have been made either by you or by a foreign state? Do they concern electronic data which are not subject to interception and which have to be separated and sorted out (in the requested or in the requesting state)? (See already above question 10.)

    b) Have you otherwise asked or otherwise been asked to guarantee that the received data must be dealt with in a certain way (e.g. kept secret, used only for specific purposes, be deleted after a certain time period)? Did you demand such guarantees when you granted mutual assistance and transmitted intercepted data to a foreign country?

27. Under some mutual cooperation agreements (e.g. EU-MLA-requests for electronic interception), a requesting state can ask the requested country to comply with formalities and procedures of his law (e.g. demanded by his law for using the data in court) (as it is possible according to Art. 9 para. 2 Directive regarding the European Investigation Order or Art. 4 para. 1 MLA Convention EU 2000)? Did you make or receive such demands when requesting mutual assistance for electronic interception? What types of requests have been made? Have these demands been fulfilled?

28. How effective is it to get communication intercepts by joint / parallel investigations in the foreign country?

29. What role do informal channels of cross border police and judicial cooperation play with regard to interception of communication?

30. Are the officials involved in electronic interception sufficiently familiar with the applicable legal framework? Is there a significant discrepancy between the legal requirements and the interception practice?

31. Are there any specific problems with or restrictions on using data stemming from a foreign interception of communications in criminal *(court) proceedings* in your country? Does the use of this data depend on the legality of interception according to the foreign legal order or according to your own legal order?

32. Is the described MLA-system for the interception of telecommunications only used for the prosecution of past crimes or also for the prevention of future risks? If yes, on which basis is it done? If not, do you consider it necessary?

33. The internet enables a wide range of online interception and searches not only on a country's own territory but also with respect to computer and network nodes located in foreign countries. To what extent is it legally, technically, and practically possible in your country to access (communication) data in a foreign country without the involvement of foreign agencies? In which cases is this practiced in your country for criminal law purposes by the police or prosecution services (e.g. access to publicly available websites on a foreign server, access to not publicly available services like e-mail accounts or Cloud services, cases where the location of a server is not known, emergency situations, other cases)? What types of cases have these been? Were these cases followed by a subsequent notice (e.g. as provided for specific cases by Art. 20 MLA Convention EU)?

34. Do you have any legislation or guidelines on or any practical experience with the interception of satellite telecommunications transmitted from planes or vessels in international airspace or waters?

35. Did you have any court decisions limiting mutual legal assistance for *constitutional grounds* either in general or with respect to the interception of telecommunication?

36. In which laws and guidelines are the cooperation issues discussed in this interview regulated?

37. Are there any reform discussions (legislative or other) with respect to the current cooperation framework? What are the motives?

IV. Specifics of EU Cooperation

38. Are there practical differences between cooperation with EU and non-EU states?

39. To which extent are incoming MLA requests for electronic interception based on
(a) Art. 30 or 31 of Directive 2014/41/EU regarding the European Investigation Order;

(b) Art. 18, 19, and 20 of the EU Convention on Mutual Assistance in Criminal Matters of 2000 (countries that are not part of the Directive regarding the EIO, e.g. Denmark, Norway, and Iceland)
(c) the MLA Convention of the Council of Europe of 1959,
(d) bilateral agreements, and
(e) national law on international cooperation in criminal matters?
Does the respective basis of MLA-requests play a role for your practical work?
How is the situation with outgoing MLA-requests?

40. To which extent are the incoming MLA requests for electronic interception to your country executed by
(a) direct and automated transfer of intercepted data ("immediate transmission" as e.g. foreseen in Art. 30 para. 6 lit. a) Directive EIO / Art. 18 para. 1 lit. a MLA Convention EU), or
(b) the traditional regime of interception, recording, and subsequent transmission of data (lit. b of said articles)?
How is the situation with outgoing MLA-requests?

41. To which extent do incoming MLA requests for electronic interception concern
(a) subjects or access points in your country,
(b) technical support for interception in the requesting state, or
(c) technical support for interception in third countries
(e.g. as foreseen in Art. 18 para 2 a–c MLA Convention EU)?
How is the situation with outgoing MLA-requests?

42. Do you have any experience with notifications from foreign LEAs in the cases when no technical assistance is needed (situations as described in Art. 31 Directive EIO, Art. 20 MLA Convention EU)?

43. In addition to the language(s) of your state, is there an additional language that may be used for completing or translating the EIO (as foreseen in Art. 5 para. 2 EIO)?

44. What should be done – in general or within the EU – for making international interception procedures more efficient? What should be done in order to protect civil liberties in such procedures better?

V. Statistics

45. Are there any statistics on the use of electronic interception and/or the access to stored communication (esp. in the criminal justice system, but – if available – also in the other above regimes)?

46. a) Could you provide a rough estimation on the extent of requests for electronic telecommunication interception which your country **demands** from other countries? How many go to Germany?

    b) Could you provide a rough estimation on the extent of MLA-requests for interception of telecommunication which your country **receives** each year from abroad? How many are from Germany?

VI. Legal Regulation

Our study also requires a more detailed analysis of the legal framework of your country on electronic interception. Could you please help us later to go through our legal questionnaire (after a pause or tomorrow or even later in writing?). If time is short it is possible to deal only with the main questions (printed in bold).

Max Planck Institute for Foreign
and International Criminal Law
79100 Freiburg i.Br. / Germany
– Department for Criminal Law –
Prof. Dr. Dr. h.c. mult. Ulrich Sieber

International Legal Cooperation in the Interception of Telecommunication

– Structure and Questionnaire for the National Country Reports –

(INTLI-Research Doc. No. 3 – V 2.0)

Function of this Document

The INTLI-study of the Max Planck Institute for Foreign and International Criminal Law in Freiburg/Germany aims to improve mutual legal assistance for the interception of telecommunication (INTternational Legal Interception – INTLI). Special focus lies on the question, whether and how intercepted data can be exchanged in real time between different national (esp. European) criminal justice systems, thus making investigation and prosecution of serious crimes more effective without undue limitations of the civil liberties of citizens. The structure of the expected general report will be specified in accordance with the progress of the study in INTLI-Doc. No. 1.

The research is based on a study of the respective national laws and the relevant international instruments ("law in the books") and on the present practices in the various national criminal justice systems ("law in action"). This twofold approach is reflected in two questionnaires that focus on legal and practical aspects of lawful interception, and, thus, complement each other: The practice of the law in action is investigated by interviews with practitioners (esp. from LEAs and Government) in the field of telecommunication interception; these interviews are structured and harmonized by the on hand interview guide draft INTLI-Doc. No. 2. **The law in the books is analyzed by country reports on the national legal situation following a common structure and common questions described in draft INTLI-Doc. No. 3.**

Contents of INTLI Doc. No. 3:

Structure and Questionnaire for the National Country Reports

Object, Aim, and Method of the Project

I. Object of Research

Technical and social changes in electronic communication and other internet services create new opportunities and new risks for *using computer data in criminal investigations*, esp. with respect to the interception of electronic communication and the access to stored communication data. This leads to new challenges for the traditional coercive powers in criminal procedural law, for the respective international cooperation, and for the protection of civil liberties of citizens. This is esp. the case for the subject matter of the present research in the field of criminal justice: the *interception of electronic communication in a global world*.

II. Aim of Research

The **main practical aim of the present study and the following questionnaire is to analyze the chances of a *cooperation model* in the field of electronic interception, by which the judicial institutions** of one country can directly access in real time electronic communication data in a foreign country. This practical goal requires two additional objectives in the area of more fundamental research: First, a comparative analysis of *national legal provisions on interception* of electronic communication and access to related data and services. And second, an analysis of the present *cooperation regime for transnational interception* of electronic evidence, esp. with respect to the results of telecommunication surveillance.[1]

III. Method of Research

The analysis of the legal questions to be solved will be based primarily on an investigation of the respective international instruments as well as a systematic comparative analysis of the national laws in the books. This normative analysis of the various national laws is based on the topics and questions described in this paper (INTLI Research Doc. No. 2). It will be amended by additional interviews with practitioners esp. from the law enforcement community which will also describe the existing problems and the law in action (INTLI Doc No. 3).

---

[1] Such a basic approach is necessary e.g. since countries can only provide legal assistance by activities permitted to them by their national laws and – in addition - can make their consent to mutual assistance subject to any condition which would have to be observed in a similar national case. Furthermore this information is needed as a basis for national and international law reform (esp. for the development of new internet-based international cooperation regimes).

IV. Scope of the Project

In the present questionnaire, the *definition of the object of interception*, i.e. electronic communication, is to be understood in a wide sense and *extended beyond the traditional concept* of communication between persons in order to obtain a broad working hypothesis especially to consider the two following developments:

(1) In today's information society, communication is no longer limited to communication between persons, but includes communication between persons and machines. Thus, when defining electronic communication for the purpose of this research, it is irrelevant whether the sender or the recipient of communication are persons or computer systems. The scope of this research includes – under the term of *electronic communication* – e.g. also communication between a person (behind a computer) and a website, a person and a server on which one's own data is stored (e.g. cloud servers), or between two machines (e.g. data transmitted within the "internet of things" e.g. between two cars). It also does not matter whether the object of transmission, i.e. data, represents audio or video content, tracking data, keystrokes, or any other kind of signals. Based on this broad working definition of "*electronic communication*" it is then up to each country report to explain, which of these broadly defined communication processes and data can be the object of the respective national legal provisions on the interception of telecommunication data.

(2) Furthermore, in IT-Systems the differentiation between *storage and communication* of data is losing its practical importance (as is illustrated by mail stored on the servers of a provider before being downloaded by the recipient). Since electronic communication is defined by the requirement of *transmission of data* between at least two persons or computer systems, this technical definition of communication does not directly apply to the access of investigation authorities to stored data e.g. by using the traditional provisions of search and seizure or remote forensic software (so-called online-search). However, since data of electronic communication can be often accessed "indirectly" by these traditional or new access provisions before, during or after their transmission, these "access provisions" for stored data must also be considered in the following analysis (as far as they are directed to data which will be, are, or have been transmitted between two persons or computers, see below).

V. Special Emphasis

The following questions on the interception of electronic communication in European criminal justice include new topics, some of which are not yet clearly regulated or decided by criminal procedural law in many European states. For that reason, country reporters are asked, when responding to the following questions, to indicate also if questions are

clearly decided or controversially disputed or not yet dealt with in their country; they should also refer to actual reform projects. If adequate, they should also indicate whether answers to the following questions are based on the wording of the respective laws, constitutional requirements, jurisprudence, literature, present practice (law in action), and/or on their own evaluation. It would also be helpful if country reporters would cite the decisive parts of relevant legal provisions in their answers in short and also collect the complete legal provisions and main decisions of jurisprudence in an appendix.

Proposed Topics and Common Structure of the Country Reports

Questions to Be Answered within the Above Structure

A. Introduction: General Background of the National Legal System

Question 1: Basic architecture of the legal system

The interception of electronic communication has become a major instrument for criminal investigation, prevention of future dangers, and information gathering of intelligence agencies. In many European countries, such an interception of electronic communication is possible under different legal regimes, esp.: (repressive) criminal law, (preventive) police law, and intelligence (or state security) law.

a) Which of these (or other) legal regimes exist and provide coercive powers for interception of electronic communication in your country?

b) What are the respective legal provisions for intercepting electronic communication in the abovementioned regimes? How far do the prerequisites for the interception of electronic communication differ between these regimes (please provide only a short overview, no details)?

c) Which authorities are technically enforcing the respective interception measures under the above regimes in your country? Is the technical implementation done by state agencies (also based on cooperation duties of IP-providers) or is it partly or completely outsourced to private companies? Are there centralized institutions, e.g. for the whole territory of the state or the country, either for one or for various of the above regimes?

d) Are the various institutions responsible for these regimes and functions separated from each other (as e.g. in Germany) or are the interceptions carried out by joint agencies (such as the English police being responsible for both prevention and repression, or the American FBI simultaneously performing duties as both a preventive and repressive police institution as well as an intelligence agency)?

e) Can the results of specific interception measures (not strategic mass surveillance) under these different regimes be exchanged between the competent authorities and regimes within your country (e.g. between national intelligence agencies and the national police)? (Please provide only a short overview, no details.)

f) Can intercepted data be exchanged with competent authorities in other countries (in particular, between intelligence agencies)? (Please provide only a short overview, no details.)

Question 2: Statistics on electronic communication interception

a) Scope of *national* interceptions in your country: Are there any statistics on the use of electronic interception and/or the access to stored communication (esp. in the crimi-

nal justice system, but – if available – also in the other above regimes)? If possible, please indicate the object of these statistics (esp. its definition of interception) and the number of interception incidents per year by providing absolute numbers and/or numbers per inhabitants and/or numbers per electronic communication-access points and/or electronic communication calls. Please be aware that a low number of interceptions under criminal law can be compensated to a certain degree by a high number of interceptions under intelligence or police law if there are no limitations on data flows between these systems.

b) Is there any obligation for enforcement agencies or courts to report statistics to a central institution, e.g. the Ministry of Justice?

B. Constitutional, Legal, and Doctrinal Safeguards for the Interception of Electronic Communication

Question 3: Specific constitutional and non-constitutional protection for electronic communication and for computer-stored data

a) Does your country have *constitutional* safeguards for the protection of telecommunication data (such as the secrecy of telecommunication[2]) and/or for personal data stored or transmitted in computer systems (e.g. the right to privacy, the right of informational self-determination on personal data,[3] or the integrity of information systems[4])?

b) Does your country provide a *constitutional* "principle of proportionality and necessity" and to what extent is it relevant for coercive powers in criminal procedural law, both in general and – especially – in the field of interception of electronic communication?

c) Are there other (non constitutional) legal safeguards for the protection of the secrecy of telecommunication (e.g. criminal laws), the protection of personal computer-stored data (e.g. special protective rules for the *collection and transfer* of personal da-

---

[2] The secrecy of telecommunication refers to a principle that aims at protecting the incorporeal transmission of information from a sender to an individual recipient using technical devices.

[3] In some countries, the principle of "self-determination on personal data" requires that citizens have a right to decide on the collection, storage, use, and disclosure of their data; the use of personal data must therefore be either regulated by law or be based on an informed consent of the respective person.

[4] The trust in the integrity of information systems is meant to protect information systems from impacts on their confidentiality, integrity or availability, esp. by means of the use of remote forensic software.

ta by the principle of "purpose limitation of personal data."[5]) or special contents transmitted by telecommunication (such as professional secrets, business secrets)?

d) What are the consequences of these safeguards for the interception of (electronic) communication? Are there legal safeguards to ensure effective protection of the intercepted data against the risk of abuse and against any unlawful access and use of that data?

Question 4: Principles for the definition of coercive powers in criminal procedural law

a) Are there any constitutional or doctrinal rules for the precise definition or interpretation of coercive powers in criminal procedural law (such as the nullum crimen sine lege principle in substantive criminal law,[6] or the principle of precise parliamentary enactment of public powers[7])? Is an analogous application of coercive powers possible?[8]

b) Are coercive powers in your criminal procedural law based on differentiated, precise, and specific provisions? Or does your country have a general clause for coercive powers, either in general or for minor cases? Are there other important (esp. protective) aspects behind the systematization and definition of the coercive powers in your criminal procedural law?

C. Coercive Powers for Accessing Electronic Communications Data in Criminal Procedural Law

I. Overview of the legal framework and the respective provisions in criminal procedural law

Question 5: Framework for accessing electronic communications data in criminal justice

Please give a short overview on the system of criminal procedural laws which can be used for intercepting electronic communication and for otherwise accessing electronic com-

---

[5] In some countries, the principle of "purpose limitation of personal data" states that data can be collected by an agency for a specific purpose and be used by and transferred to another agency for another purpose only if this is permitted by law and if this is necessary.

[6] In substantive criminal law, the principle "no crime without legal definition" requires inter alia that criminal statutes must be defined precisely by the legislator before the commission of a criminal act can be assumed.

[7] The principle of precise parliamentary enactment of public powers requires that all infringements of civil liberties must be based on precise laws.

[8] This means that a provision can be applied to a situation that is not justified by the provision's wording, but by its purpose.

munications data for the purpose of criminal investigations and which are described in more detail infra. Are additional general clauses applicable?[9]

II. Interception of content of electronic communication data in criminal procedural law

Question 6: Respective provision

Most countries have one main provision in criminal procedural law (often specified by additional legal provisions) dealing with the interception of the content of communication in transmission. The following questions refer to this main provision (or – if available – to the main provisions), whereas provisions primarily concerning other specific purposes (e.g. search and seizure of stored data) should be dealt with in section D, questions 17 to 19 only. Please provide the provision and cite the wording of its core part (in English).

Question 7: Object of interception

a) How is the object of interception defined in the above provision of your criminal procedural law (e.g. as "telephone communication", "electronic communication", "electronic communication between persons", …)?

b) Which of the following contents of traffic are covered by the respective provisions and can be captured under your criminal procedural law? Does it include e.g.:
   - analogous communication (voice and data) via landlines?
   - IP-traffic of a person-to-person-communication?
   - IP-traffic between a person and an automated information system (such as communication with a webserver while downloading a website)?
   - IP-traffic between a person's computer and their data storage in a cloud or other remote storage of data processing systems (is this covered by "communication", as defined in the above main legal provision, between the user and the cloud provider or as an internal activity within the private storage devices of the user which is comparable with the use of a single internal storage device)?
   - IP-traffic between two independent computer systems (e.g. between an automated machine and its computer-based automated control center, esp. in the "internet of things")?
   - any other options?

[9] Legal provisions of intelligence law (state security law) and preventive police laws should be mentioned only in question 1 above.

c) Does the respective main provision for content interception cover electronic communication data only during their *transmission* or also when the respective data are *stored* before, during, or after this process of transmission (e.g. e-mail drafts or sent e-mails, e-mails stored by the provider, received e-mails stored by the recipient or completely web-based communication such as in social networks)? If so, are there any special criteria that stored e-mails or messages must fulfill in order to be covered by the main provision for content communication interception (is there e.g. a differentiation between read and unread e-mails or messages)?

d) If there are no explicit rules on these questions: Is there a discussion on respective constitutional requirements? Could constitutional reasoning influence these discussions in the future?

Question 8: Privileged information

a) Does your criminal procedural law (or any other law) provide specific safeguards excluding particular types of information from electronic communication interception, e.g.
   - communication under professional secrecy, such as communication between an attorney-at-law and a client, a medical practitioner and a patient, a priest and a parishioner, journalists' communication, etc.?
   - communication protected under the law regulating financial and banking secrecy?
   - communication in a "core area of private life" (e.g. prayers, communication during sexual activities, diaries, …)?
   - any other type of communication?

b) If information is thus privileged, what consequences does this entail, e.g.
   - interception is not possible and has to be suspended immediately (and can be turned on later again?) by the police?
   - interception can be continued and critical records have to be checked and erased immediately or later by the police?
   - information can be used in certain cases (if so in which)?
   - any other options?
   - are there (technical) differences between handling analogous and digital communication?

c) Who has to decide at which stage of the interception and in which way these privileges and/or the analysis of the respective captured information has to be conducted, e.g.
   - the magistrate issuing the respective warrant?
   - the prosecutor?
   - the executive police agent or his technical assistants?
   - the internet provider before handing over the respective data?

d) If there are no explicit rules on these questions: Is there a discussion on respective constitutional requirements? Could constitutional reasoning influence these discussions in the future?

Question 9: Mode of interception

a) Which of the following *modes of interception* are state agencies *legally entitled* to use under criminal law in order to intercept the content of electronic communication?
   - Ordering access providers to extract and surrender specific communication?
   - Intercepting specific communication themselves and without recourse to third parties (e.g. by interception of cables, interception of a WLAN, use of remote forensic software, satellite communications)? Are there in the latter case any rules in your national law for the situation when the intercepted device is located in another country or if the location of the device is unknown?

b) Which *types of accompanying investigative measures* are permitted in your country's main provision on electronic interception under your criminal law for the interception of electronic communication (e.g. clandestine access to houses in order to place equipment, hacking techniques, use of key loggers)?

Question 10: Specific cooperation duties of internet providers

a) Which internet providers can be ordered by judicial warrant to execute interception orders, e.g.
   - access providers on the IP-transport level?
   - infrastructure providers working on the IP-transport level (such as central network nodes without direct contacts to the users)?
   - providers working on the IP-application level providing social interaction (e.g. e-mail or phone services, social networks) or data storing/processing services (e.g. cloud-providers or IoT services, e.g. data transmitted from sensors) (see also question 18 below)?

b) How does your law describe and regulate the cooperation duties of these providers?

c) Are there any provisions requiring communication providers to follow certain rules on interception capabilities in their networks, e.g. to purchase and install special equipment for intercepting communication, to ensure the technical capability to intercept communication, and/or to provide access to stored data for the police (not the powers to compel interception itself), protocolling duties, etc.?

d) Which norms exist concerning the technical aspects of the internet providers' transfer of intercepted data to the police, e.g. with respect to

- formats and protocols?
- transport channels?
- security measures?
- encryption?

e) Are there norms or is there any other regulation stipulating technical aspects of the internet provider's transfer of intercepted data to authorities in a foreign country (e.g. in the context of mutual legal assistance)?

Question 11: Formal prerequisites of interception orders

a) Which authority (e.g. judge, prosecutor, head of police) can authorize and which authorities can apply for interception orders
   - under normal circumstances?
   - in case of (which types of) emergency?

b) Are there any formal requirements for the application (e.g. oral presentation before the approving authority, written submission)? Which information must be contained in the order? Does it need to give a reason?

c) On grounds of what evidence is the applicant's case presented to the competent authority (e.g. simple application, oath, submission of investigative files)?

Question 12: Substantive prerequisites of interception orders

a) Which degree of suspicion for a past crime (or – in some countries – which degree of future danger or risk) is necessary for an interception order?

b) Which crimes or (dangers) can justify an interception order? Please also state whether the potential or the likely sentencing range serve as (additional?) limiting criteria.

c) In case of suspicion of crime, who can be subject to an interception order (e.g. suspects, their intermediaries, their communication partners, specific devices)? Can a legal person be subject to an interception order?

d) Is it possible that an interception order, for the purpose of a *criminal investigation*, is not directed against a particular individual, against particular premises, or against a specific device, but instead targets particular communication content (e.g. through the automated use of certain trigger words)?

e) Is there a specific requirement regarding the likelihood that the anticipated evidence will actually be obtained by means of the requested interception?

f) For the admissibility of electronic communication interception does your law require that other – less intrusive – means of investigation first be tried unsuccessfully or be considered unlikely to be successful?

g) Besides consistency with the aforementioned requirements, is there an additional obligation for the authorizing authority to verify that the interception is proportionate to the seriousness of the offence in the individual case? Which particular factors will most likely preclude proportionality?

h) Is an interception order required when one of the parties to the communication has consented to the interception?

Question 13: Validity of interception orders

a) What is the maximum length of an interception order
   - under normal circumstances?
   - in case of emergency?

b) How often and to which maximum duration can it be prolonged?

c) Does the renewal or prolongation of the interception warrant follow the same procedure as the initial application for an interception?

d) Can an interception order be revoked and under which circumstances?

e) Is there an obligation for the relevant authority or any other body to revoke the authorization when a subsequent lack of substantive prerequisites becomes apparent?

f) Must the interception be halted if it reveals information pointing to the commission of offences not anticipated by or not mentioned in the interception order?

Question 14: Recording and reporting requirements

a) Are there protocolling duties?

b) Are there (obligatory) reports on progress of interception and final reports that have to be submitted to the judge/any other body (and at which time intervals)?

c) Are there any requirements to destroy the records which are not related to the aim of the interception warrant, or which are not needed as evidence (any more)? Who is responsible for the destruction of the records and what is the procedure?

Question 15: Notification requirements and remedies against interception orders

a) Is there a duty of the investigative authorities to inform intercepted persons about an interception, e.g. as soon as this is possible without endangerment of the investigation or after completion of the investigation? If so, to what extent is such notification practiced?

b) Does the person subject to an interception order have remedies against an illegal or illegally performed interception, in case he/she becomes aware of the interception?

c) In case of judicial review or other remedies: are there procedural particularities to such a review (e.g. *in camera* proceedings, limits on the state's disclosure obligations, need to give reasons for a dismissal)?

d) Are officials conducting interceptions illegally subject to particular sanctions? Can you state the frequency with which such cases arise or sanctions are imposed?

e) Is there any independent monitoring authority that has the power to control the interception of communication and make sure that it is carried out in accordance with the legal requirements/legal authorization?

Question 16: Confidentiality and reliability requirements

a) Is there a specific obligation for internet providers to keep their support measures confidential?

b) Are there specific (criminal?) sanctions for infringements of this obligation?

c) Are there particular obligations for the person conducting the interception to maintain the integrity and reliability of the material obtained (e.g. sealing the data storage medium, transmission of intercepted data to a judicial authority immediately following the interception, producing transcripts in the presence of defense lawyers)?

III. Interception of *traffic data* for criminal justice

Question 17: Interception of traffic data and subscriber data

a) Please provide the relevant provisions and, if possible, cite the wording of their core parts (in English).

b) What are the requirements (esp. safeguards) for accessing traffic data in your country? Is this possible by way of an automated on-line procedure?

c) What are the requirements for accessing subscriber data in your country? Is this possible by way of an automated on-line procedure?

d) Subject to which rules can the attribution of dynamic IP-addresses to specific users at a given time be obtained from internet providers? Is this possible by way of an automated on-line procedure?

e) Does your country require internet providers to retain subscriber information?

f) Does your country require internet providers to retain traffic data? How long must data be stored? What kind of data must be stored (e.g. phone numbers, e-mail addresses, date and time of a connection, IP-addresses)?

Question 18: Identification of the device ID of a mobile end terminal and its card number

a) Does your country have such a provision? If yes, please give a short description of this provision, esp. with respect to the information to be obtained.

b) Or can such activities be justified by other provisions (e.g. the general provision on interception)? If so, please give a short description of this provision.

IV. Applying "access-to-stored-data provisions" to electronic communication processes

Question 19: Online-search by remote forensic software (including specialized norms on source electronic communication interception)

Does your country have a provision on the use of remote forensic software or similar provisions? If so, please give a description of this provision, esp. with respect to the activities permitted (e.g. hacking, keylogging), the data which can be accessed (all stored data or only electronic communication data), the option to use this measure without the knowledge of the persons concerned, the duties to disclose the measures at a later stage, the regional scope, limitation of the scope (e.g. crimes that can be investigated with ordering this measure, additional safeguards, and others).

Question 20: Search and seizure for stored electronic communication data

a) To what extent is this approach possible in your legal system?

b) Is this option provided for in other ways than by using the general powers to intercept communication in form of the aforementioned central provisions for the interception of electronic communication or do the more restricted provisions on electronic communication interception (as the more specialized lex specialis) supersede or replace the provisions on search and seizure?

c) Do the safeguards and requirements for the interception of communication differ for interception and access to stored data? Does communication in transmission have a higher degree of legal protection (e.g. is information in transmission better protected

than the same information the second after its transmission has terminated and it has been stored)?

d) Must the access to stored communication be performed as an open measure or can it be performed in a clandestine way? If it has to be performed openly, does it depend on the awareness of the suspect and/or on the awareness of the provider?

Question 21: Production order and decryption order

a) Does your country have a *special regulation* providing cooperation duties for decoding encrypted data or to hand over the necessary passwords in one or more of the following forms:
   - as an independent general provision?
   - in connection with the provisions on search and seizure and/or production orders?
   - in connection with the provisions on interception of electronic communication?

b) Who is the subject of the duty to provide the encryption key in the cases stated above (e.g. anybody, a communications provider, …)? Are these provisions also applicable to the suspect of the investigation? If the suspect has a duty to decrypt or to provide a key, how does this correlate with the prohibition on self-incrimination in your legal doctrine? If possible, please make reference to any specific legal provision or court decision(s) on this matter.

Question 22: Others

Does your country have additional/other coercive powers which might be relevant for accessing electronic communication data either during transmission or in stored form before, during, or after transmission (e.g. a general clause)?

V. Use of electronic communication data in court proceedings

Question 23: Specific regulations on use

a) Are there specific rules for using intercepted electronic communication data in court proceedings (please only refer to rules especially designed for admissibility of intercepted or stored electronic communication data as evidence in the court and not to general rules)?

b) In which form is intercepted material introduced as evidence in criminal proceedings (transcripts, audio recordings, witness testimony)?

c) Which consequences does the non-observance of the aforementioned formal and substantive prerequisites have on the admissibility as evidence?

d) Can intercepted data be used for the prosecution of offences other than the offences mentioned or anticipated in the interception order?

e) Can intercepted data be used for the prosecution of individuals who were not subject of the underlying interception order?

f) Is intercepted data obtained from outside the criminal justice system (e.g. intelligence services, non-judicial police forces) admissible as evidence in criminal proceedings?

g) What are the rules on the admissibility of intercepted data obtained from foreign jurisdictions?

h) To what extent can the accused challenge the probity of intercepted evidence? Please also state relevant disclosure obligations of the prosecution (e.g. regarding the technical means used for the interception).

D. Exchange of Intercepted Electronic Communication Data between Foreign Countries

Question 24: Legal Basis for mutual legal assistance

a) What is the legal basis on mutual legal assistance applicable for the interception of electronic communication? E.g.
– has the Directive 2014/41/EU regarding the European Investigation Order been implemented in your country (esp. Art. 30, 31)?
– which international conventions are applicable in your country? E.g. the Convention on Mutual Assistance in Criminal Matters between the member States of the European Union of 2000 (esp. with Art. 17-21),[10] the European Convention on Mutual Assistance in Criminal Matters of 1959 (esp. with its general clause in conjunction with the CoE Committee of Ministers' Recommendation No. R (85) 10), the Convention on Cybercrime (esp. with Arts. 23–35), the United Nations Transnational Organized Crime Convention of 2000 (esp. Art. 18), etc. ?

b) Does your country have additional bilateral treaties on mutual legal assistance with Germany or with the EU covering interception of electronic communication? How is interception of electronic communication regulated therein (especially in compari-

[10] It should be noted that this convention has not yet been ratified by Greece, Italy, Croatia, and Ireland.

son with the abovementioned EU Directive on the European Investigation Order / the EU Convention of 2000 or other conventions ratified by your country)?

c) Does your country have additional national regulation on mutual assistance and interception of electronic communication in criminal matters beyond the ratified treaties (e.g. in general national rules on mutual legal assistance)? What is the content of the respective national laws with respect to electronic interception (either in general rules on mutual assistance or in specific regulations on interception)? Does this legislation enable non-treaty based mutual assistance for the interception of electronic communication (e.g. for specific countries or in addition to the treaty-based legal regimes)?

d) Beyond legal provisions: Are there specific guidelines for the competent authorities regarding the cross-border interception of telecommunications?

Question 25: Procedures and execution of requests

a) If your country receives a foreign request for the interception of telecommunication: Which authorities are responsible for granting the request and which authorities are responsible for executing it? What is the respective procedure prescribed by your national law? What are the rules for protecting the individual/person concerned by a cross-border interception measure, e.g. remedies, notification obligations, etc.?

b) Is there a duty to filter out or to delete privileged information (see question 8) before your country transmits the results of an interception measure to a foreign country? Would this obligation also apply within a real-time transmission of intercepted data to a foreign country?

c) Does law or case law in your country provide for the possibility to make the transfer of the intercepted data subject to conditions or require assurances from the requesting state? If yes, what is the contents of these conditions and/or assurances?

c) In the opposite case (if your state is requesting interception of electronic communication in a foreign country): Which authorities send out the requests? If you later receive the results of the requested interception measure, do you have a duty to filter out or to delete information which could not be intercepted according to the laws of your state (or even to the law of the sending state) due to a legal privilege (see question 8)?

d) In what cases is it allowed to store communications that have been intercepted after data has been transferred (immediately or subsequently) to the requesting state (e.g. in case of parallel investigations, for sampling inspection, data protection purposes, for general purposes, …)?

Question 26: Real-time transfer of communications data

a) Looking at the current design of your national legal regime on telecommunications interception as well as at your national law on mutual legal assistance, to which extent is a *direct extraction and transfer* of intercepted electronic communications data among foreign police and judicial authorities already possible under your domestic law? Can a foreign police and judicial authority directly address communication providers in your country in view of requesting the extraction of communications data? Can communications providers in your country directly transfer communications data to a foreign authority without involvement of a domestic authority?

b) What technical, legal, and organizational reform measures (national and/or international) would be necessary to enable such "real time cooperation" in the field of interception measures or to increase its effectiveness?

c) If applicable, how will the recently adopted European Investigation Order affect MLA in the area of intercepted communication? Did/does your legislator anticipate any challenges with regard to its domestic implementation? Did you implement any specific provisions on the cross-border interception of telecommunications on the occasion of implementing the European Investigation Order?

Question 27: Statistics

Are there any statistics or information of your Ministry of Justice on the extent of MLA-requests for electronic telecommunication interception? If yes: How many MLA-requests for interception of telecommunication does your country receive each year from abroad? How many are from Germany?
How many of such requests does your country send to foreign countries/to Germany per year?

Authors and Co-Authors

Prof. Dr. Dr. h.c. Lorena Bachmaier Winter (Madrid)

Assoz. Prof. Dr. Christian Bergauer (Graz)

Dr. Diana Bernreiter (Graz)

Gertjan Boulet (Brussels and Seoul)

Niels van Buiten (Rotterdam)

Prof. Iain Cameron (Uppsala)

Asst. Prof. Dr. Roberto Flor (Verona)

Dr. Sebastian Gölly (Graz)

Doc. dr. sc. Marko Jurić (Zagreb)

Aare Kruuser (Tallinn)

Elif Mendos Kuskonmaz, Ph.D. (Portsmouth)

Prof. Dr. Paul De Hert (Brussels and Tilburg)

Dr. Estelle De Marco (Montpellier)

Assoc. Prof. Dr. Stefano Marcolini (Varese)

Patrick Köppen (Wiesbaden)

Dr. Nicolas von zur Mühlen (Berlin)

Asst. Prof. Katalin Parti, Ph.D. (Blacksburg)

Doc. JUDr. Radim Polčák, Ph.D. (Brno)

Assoc. Prof. Dr. Dr. h.c. Sunčana Roksandić (Zagreb)

Prof. Dr. Gabriele Schmölzer (Graz)

Prof. Joseph J. Schwerha IV (California, PA)

Catherine Smith (Canberra)

Dr hab. Sławomir Steinborn (Gdańsk)

Prof. Dr. Dr. h.c. mult. Ulrich Sieber (Freiburg)

Dr. Stanisław Tosza (Luxembourg)

Dr. Tatiana Tropina (Leiden)

Dr. Benjamin Vogel, LL.M. (Cantab.) (Freiburg)

Pedro Verdelho (Lisbon)

Thomas Wahl (Freiburg)

Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht

The main research activities of the Max Planck Institute for Foreign and International Criminal Law are published in the following six subseries of the "Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht" (Research Series of the Max Planck Institute for Foreign and International Criminal Law), which are distributed in cooperation with the publisher Duncker & Humblot:

- "Strafrechtliche Forschungsberichte" (Reports on Research in Criminal Law)
- "Kriminologische Forschungsberichte" (Reports on Research in Criminology)
- "Interdisziplinäre Forschungen aus Strafrecht und Kriminologie" (Reports on Interdisciplinary Research in Criminal Law and Criminology)
- "Publications of the Max Planck Partner Group for Balkan Criminology"
- "Series of the Max Planck Institute for Foreign and International Criminal Law and Bahçeşehir University Joint Research Group"
- "Sammlung ausländischer Strafgesetzbücher in Übersetzung" (Collection of Foreign Criminal Laws in Translation)

These publications can be ordered from the Max Planck Institute at <www.mpicc.de> or from Duncker & Humblot at <www.duncker-humblot.de>. Two additional subseries are published: "research in brief" contains short reports on results of research activities, and "Arbeitsberichte" (working materials) present preliminary results of research projects. These publications are available at the Max Planck Institute.

Detailed information on all publications of the Max Planck Institute for Foreign and International Criminal Law can be found at <www.csl.mpg.de>.

Die zentralen Veröffentlichungen des Max-Planck-Instituts für ausländisches und internationales Strafrecht werden in Zusammenarbeit mit dem Verlag Duncker & Humblot in den folgenden sechs Unterreihen der „Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht" vertrieben:

- „Strafrechtliche Forschungsberichte"
- „Kriminologische Forschungsberichte"
- „Interdisziplinäre Forschungen aus Strafrecht und Kriminologie"
- „Publications of the Max Planck Partner Group for Balkan Criminology"
- „Series of the Max Planck Institute for Foreign and International Criminal Law and Bahçeşehir University Joint Research Group"
- „Sammlung ausländischer Strafgesetzbücher in Übersetzung"

Diese Publikationen können direkt über das Max-Planck-Institut unter <www.mpicc.de> oder über den Verlag Duncker & Humblot unter <www.duncker-humblot.de> erworben werden. Darüber hinaus erscheinen in der Unterreihe „research in brief" zusammenfassende Kurzbeschreibungen von Forschungsergebnissen und in der Unterreihe „Arbeitsberichte" Veröffentlichungen vorläufiger Forschungsergebnisse. Diese Veröffentlichungen können über das Max-Planck-Institut bezogen werden.

Detaillierte Informationen zu den einzelnen Publikationen des Max-Planck-Instituts für ausländisches und internationales Strafrecht sind unter <www.csl.mpg.de> abrufbar.

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Selected criminal law publications:

S 172 *Jan Caba*
Obstruction of Justice at the International Criminal Court
A Comparison with the United States, Germany and the International Criminal Tribunal for the Former Yugoslavia
2021 • 796 Seiten • ISBN 978-3-8611 -764-1 € 58,00

S 171 *Angélica Romero Sánchez*
Ermittlungen gegen Organisierte Kriminalität
Ein Vergleich des deutschen und kolumbianischen Rechts
2021 • 744 Seiten • ISBN 978-3-8611 -766-5 € 56,00

S 170 *Daniel Burke*
Schutz kartellrechtlicher Kronzeugen vor strafrechtlicher Sanktion
Eine Untersuchung zu Notwendigkeit und Gestaltung einer Kronzeugenregelung im deutschen Kartellstrafrecht
2020 • 320 Seiten • ISBN 978-3-86113-768-9 € 35,00
Ausgezeichnet mit der Otto-Hahn-Medaille der Max-Planck-Gesellschaft

S 169 *Marc Engelhart/Mehmet Arslan*
Schutz von Staatsgeheimnissen im Strafverfahren
Eine Studie zur Europäischen Menschenrechtskonvention
2020 • 200 Seiten • ISBN 978-3-86113-769-6 € 32,00

S 168 *Maja Serafin*
Vermögensabschöpfung – zwischen Effektivität und Rechtsstaatlichkeit
Ein deutsch-polnischer Vergleich
2019 • 348 Seiten • ISBN 978-3-86113-771-9 € 35,00

S 166 *Nicolas von zur Mühlen*
Zugriffe auf elektronische Kommunikation
Eine verfassungsrechtliche und strafprozessrechtliche Analyse
2019 • 470 Seiten • ISBN 978-3-86113-776-4 € 44,00
Ausgezeichnet mit der Otto-Hahn-Medaille der Max-Planck-Gesellschaft

S 165 *Marc Engelhart / Sunčana Roksandić Vidlička* (eds.)
Dealing with Terrorism
Empirical and Normative Challenges of Fighting the Islamic State
2019 • 296 Seiten • ISBN 978-3-86113-777-1 € 38,00

S 164 *Yukun Zong*
Beweisverbote im Strafverfahren
Rechtsvergleichende Untersuchung zum deutschen, US-amerikanischen und chinesischen Recht
2018 • 487 Seiten • ISBN 978-3-86113-779-5 € 44,00

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Selected criminal law publications:

S **128.1.1** *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 1.1: Introduction to National Systems
2013 • 314 Seiten • ISBN 978-3-86113-822-8 € 40,00

S 128.1.2 Volume 1.2: Introduction to National Systems
2013 • 363 Seiten • ISBN 978-3-86113-826-6 € 43,00

S 128.1.3 Volume 1.3: Introduction to National Systems
2014 • 297 Seiten • ISBN 978-3-86113-818-1 € 40,00

S 128.1.4 Volume 1.4: Introduction to National Systems
2014 • 391 Seiten • ISBN 978-3-86113-810-5 € 43,00

S 128.1.5 Volume 1.5: Introduction to National Systems
2018 • 375 Seiten • ISBN 978-3-86113-785-6 € 43,00

S **128.2.1** *Ulrich Sieber / Susanne Forster / Konstanze Jarvers* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 2.1: General limitations on the application of criminal law
2011 • 399 Seiten • ISBN 978-3-86113-834-1 € 43,00

S 128.2.2 *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 2.2: General limitations on the application of criminal law
2017 • 272 Seiten • ISBN 978-3-86113-798-6 € 35,00

S **128.3.1** *Ulrich Sieber / Susanne Forster / Konstanze Jarvers* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 3.1: Defining criminal conduct
2011 • 519 Seiten • ISBN 978-3-86113-833-4 € 46,00

S 128.3.2 *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 3.2: Defining criminal conduct
2017 • 370 Seiten • ISBN 978-3-86113-790-0 € 43,00

S **128.4.1** *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 4.1: Special forms of criminal liability
2015 • 401 Seiten • ISBN 978-3-86113-803-7 € 43,00

S 128.4.2 *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 4.2: Special forms of criminal liability
2021 • ca. 200 Seiten • ISBN 978-3-86113-803-7 in Erscheinen

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Selected criminal law publications:

S **128.5.1** *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 5.1: Grounds for rejecting criminal liability
2016 • 410 Seiten • ISBN 978-3-86113-800-6 € 43,00

S 128.5.2 *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
Volume 5.2: Grounds for rejecting criminal liability
2019 • 394 Seiten • ISBN 978-3-86113-774-0 € 43,00

G 128 **Das norwegische Strafgesetz • Lov om straf (straffeloven)**
Zweisprachige Ausgabe
Deutsche Übersetzung Einführung von Karin Cornils
und Erling Johannes Husabø
2. Auflage, nach dem Stand vom 1. Dezember 2020
2021 • 297 Seiten • ISBN: 978-3-86113-817-4 € 45,00

G 127 **Das türkische Strafgesetz • Türk Ceza Kanunu**
Deutsche Übersetzung und Einführung von Silvia Tellenbach
Zweisprachige Ausgabe
2. Auflage, nach dem Stand vom 1. Januar 2021
2021 • 250 Seiten • ISBN 978-3-86113-763-4 € 45,00

Selected criminological publications:

K 191 *Kira-Sophie Gauder*
„Wieder in dieses normale zivile Leben reinkommen“
Zur Bedeutung von Normalität im Wiedereingliederungsprozess haftentlassener Sexualstraftäter. Teilstudie 1 der Langzeitstudie „Sexualstraftäter in den sozialtherapeutischen Abteilungen des Freistaates Sachsen“
Berlin 2021 • 312 Seiten • ISBN 978-3-86113- 287-5 € 37,00

K 188 *Jia Kui*
Strafrechtlicher Schutz bei häuslicher Gewalt
Eine vergleichende Untersuchung zum deutschen und chinesischenRecht
Berlin 2020 • 207 Seiten • ISBN 978-3-86113-276-9 € 32,00

K 187 *Elisa Wallwaey, Esther Bollhöfer, Susanne Knickmeier* (Hrsg.)
Wirtschaftsspionage und Konkurrenzausspähung
Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern
Berlin 2019 • 170 Seiten • ISBN 978-3-86113-275-2 € 32,00

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Selected criminological publications:

K 184 *Elke Wienhausen-Knezevic*
Lebensverlaufsdynamiken junger Haftentlassener
Entwicklung eines empirischen Interaktionsmodells (ZARIA-Schema) zur Analyse von Haftentlassungsverläufen
Berlin 2020 • 264 Seiten • ISBN 978-3-86113-282-0 € 35,00

K 183 *Katharina Meuer*
Legalbewährung nach elektronischer Aufsicht im Vollzug der Freiheitsstrafe
Eine experimentelle Rückfallstudie zum baden-württembergischen Modellprojekt
Berlin 2019 • 225 Seiten • ISBN 978-3-86113-272-1 € 35,00

K 182 *Hans-Jörg Albrecht, Maria Walsh, Elke Wienhausen-Knezevic* (eds.)
Desistance Processes Among Young Offenders Following Judicial Interventions
Berlin 2019 • 165 Seiten • ISBN 978-3-86113-271-4 € 32,00

K 181 *Maria Walsh*
Intensive Bewährungshilfe und junge Intensivtäter
Eine empirische Analyse des Einflusses von Intensivbewährungshilfe auf die kriminelle Karriere junger Mehrfachauffälliger in Bayern
Berlin 2018 • 233 Seiten • ISBN 978-3-86113-269-1 € 35,00

K 180 *Linn Katharina Döring*
Sozialarbeiter vor Gericht?
Grund und Grenzen einer Kriminalisierung unterlassener staatlicher Schutzmaßnahmen in tödlichen Kinderschutzfällen in Deutschland und England
Berlin 2018 • 442 Seiten • ISBN 978-3-86113-268-4 € 42,00
Ausgezeichnet mit der Otto-Hahn-Medaille der Max-Planck-Gesellschaft

BC 5 *Filip Vojta*
Imprisonment for International Crimes
An Interdisciplinary Analysis of the ICTY Sentence Enforcement
Berlin 2020 • 375 Seiten • ISBN 978-3-86113-280-6 € 40,00
Ausgezeichnet mit der Otto-Hahn-Medaille der Max-Planck-Gesellschaft

BC 3 *Lucija Sokanović*
Fraud in Criminal Law
A Normative and Criminological Analysis of Fraudulent Crime in Croatia and the Regional Context
Berlin 2019 • 280 Seiten • ISBN 978-3-86113-273-8 € 35,00