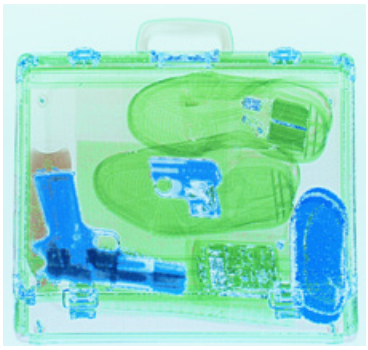
ArchiS
Architektur des Sicherheitsrechts

Marc Engelhart / Mehmet Arslan

# Security Architecture in Germany

BEITRÄGE ZUM SICHERHEITSRECHT




Max-Planck-Institut
für ausländisches und
internationales Strafrecht

# Security Architecture in Germany

Marc Engelhart · Mehmet Arslan

Freiburg im Breisgau 2020

Contributions to Security Law/7
(Beiträge zum Sicherheitsrecht/7)

Edited by Marc Engelhart

The series entitled “Contributions to Security Law” is a venue that provides open access to important research findings for a broad spectrum of professionals. The findings are the results of projects, including ongoing projects, that emerged from the Otto-Hahn-Group on the “Architecture of Security Law” (ArchiS) or are projects of individual group members. The papers are available both online in PDF format on the websites of the publication repository of the Max Planck Society (https://pure.mpg.de) and the research group (https://criminallaw.science) as well as in print.

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.



Umschlagbild: © (v.l.n.r.) kyolshin, iStock; Flying Colours Ltd., Getty Images; tirc83, iStock [obere Reihe]; NSA, www.nsa.gov; mthaler, iStock [untere Reihe]

Satz: Dorothea Borner-Burger

Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim

ISBN 978-3-86113-770-2

DOI https://doi.org/10.30709/archis-2020-7

# Contents

**Introduction** ..... 7

**I. The Precaution Paradigm of Security Policy and Changes in the Law** ..... 8

A. Technifying the Law ..... 8

B. Domestic Security as a 'Natural Problem to Solve' ..... 9

C. Emergence of Precaution-Based Security Legislation ..... 12

**II. The Precaution Paradigm of Security Policy – Evaluation under Constitutional Law** ..... 14

A. Broader Security Notion ..... 15

1. The Approach of 'Security for the Order of the State' ..... 15
2. The Approach of 'Freedom only within Security' ..... 17
3. Position of the German Federal Constitutional Court ..... 20

B. Differentiated Security Notion ..... 23

1. The approach of 'Security only within Freedom' ..... 23
2. The Proportionality Test in Security Law ..... 27
   a) General overview ..... 27
   b) Separation of the security functions in light of proportionality ..... 29

**III. Intelligence, Police, and Criminal Prosecution** ..... 31

A. Conventional Concept ..... 31

1. Intelligence Services ..... 31
   a) Structure ..... 31
   b) Federal Intelligence Service (BND) ..... 33
   c) Federal Office for the Protection of the Constitution (BfV) ..... 34
   d) Main Features of Intelligence Investigations and Differences from Preventive and Repressive Police Investigations ..... 36
2. Police ..... 40
   a) Structure ..... 40
   b) Preventive Policing ..... 42
   c) Repressive Policing ..... 43
   d) Overlaps between Preventive and Repressive Police Investigations ..... 45
   e) Main Features of Police Investigations and Differences from Intelligence Investigations ..... 47
3. Overlaps between Intelligence, Police, and Criminal Prosecution ..... 48

B. Reconfiguration in light of selected issues ..... 50
1. General Overview: Restructuring the Security Architecture ..... 50
2. Precautionary Data Retention ..... 54
3. At the Level of the Intelligence Services ..... 56
a) Federal Intelligence Service ..... 56
b) Federal Office for the Protection of the Constitution ..... 59
4. At the Level of the Police ..... 61
a) In general ..... 61
b) Precautionary wiretapping in the pre-field of concrete danger ..... 63
c) Precautionary screening in the pre-field of concrete danger ..... 64
d) Precautionary automatic licence plate recognition in the pre-field of concrete danger ..... 66
C. Main Concerns ..... 67

**IV. Intelligence Information in Criminal Proceedings** ..... 69
A. Securitization of criminal proceedings ..... 69
B. Transfer and use of intelligence information at the investigation stage ..... 71
1. Main Principles of Criminal Investigation ..... 71
2. Intelligence Information as Evidence at the Criminal Investigation Stage ..... 74
a) General framework ..... 74
b) Unsolicited information transfer ..... 76
c) Transfer on request ..... 79
3. Suspending a Transfer ..... 80
4. Use of Intelligence Information ..... 83
5. Interim Results ..... 86
C. Use of intelligence information and protection of state secrets at the trial stage ..... 87
1. Trial procedures and main principles ..... 87
a) Principles of evidence taking by the court ..... 87
aa) Constitutional framework ..... 87
bb) Statutory framework ..... 89
b) Rights of defence ..... 91
aa) Constitutional framework ..... 91
bb) Statutory framework ..... 93
2. Protection of State Secrets during Trial ..... 95
a) General framework ..... 95
b) Witness protection measures ..... 99
aa) Protection during the main hearing ..... 99
bb) Questioning of the witness outside the main hearing ..... 101
cc) Written statements and hearsay witnesses ..... 102

3. Dropping Cases over Withheld Evidence ..... 104
4. Inadmissible Evidence ..... 105
a) Illegally collected evidence ..... 105
b) Evidence collected abroad ..... 107

**Summary** ..... 109

**References** ..... 113

**List of Judgments** ..... 120
With regard to Security Law ..... 120
With regard to Criminal Procedure Law ..... 120

**List of Abbreviations** ..... 121

# Introduction

The relationship between intelligence and crime control is a key issue of domestic security law (*das Recht der inneren Sicherheit*) in Germany.[1] The ensuing question is two-pronged: first, whether or to what extent intelligence services should engage in controlling or combating crime. Second, whether or to what extent the police and criminal prosecution agencies should use the means and methods of the intelligence services to control or combat crime. These two aspects go hand in hand with the issue of introducing intelligence information at different stages of criminal proceedings.

The above questions need to be addressed due to certain developments in the new precaution-based security policy and the corresponding reconfiguration of its legal framework (I.). The legal debate surrounding the trio of security, intelligence, and crime control starts at the highest level, namely in constitutional law. In a series of judgments,[2] the German Federal Constitutional Court was called to take a stand on the crucial question of where to position the new security policy in the constitution, in particular with regard to the precaution-based concept of this policy (*Vorsorgegedanke*) due to its fundamental effect on the balance between freedom and intervention-oriented security in favour of the latter (II.). In terms of this rather conceptual question, the Court's jurisprudence defines the external boundaries of state actions relating to security and strikes a balance between the latter and freedom. German domestic security legislation in general is subject to an extensive set of requirements, inferred especially from the principle of proportionality. The Court also addresses the internal architecture of this new security legislation. To this end, the Court outlines another boundary issue, namely the limits on interactions between the three security-related branches of the federal government (intelligence, police, and criminal prosecution). The solution to this issue requires not only to identify the key characteristics of these agencies as they are conventionally understood but also to evaluate the changes that occurred as a result of expanding the security agencies' areas of responsibility or of equipping them with new methods of investigation and to adjust the changes to the constitutional requirements (III.). It is also a constitutionally guaranteed principle that the protection of basic

---

[1] The term 'intelligence' covers three aspects: intelligence as the organizations, the services; intelligence as efforts to collect information; and intelligence as a process of generating knowledge. In the following, I will attempt to clarify each time exactly what the term means.

[2] See Appendix, Judgments on Security Legislation.

rights imposes not only limits on crime control by means of the intelligence services or their methods as indicated but requires a separation of the three security branches, which the legislature must comply with. The separation rule is particularly evident in the way in which the flow of information between the intelligence services, the police, and criminal prosecution is regulated. An issue closely related to the principle of informational separation is the introduction of intelligence information at different stages of criminal proceedings. A comprehensive understanding of the scope of the inter-agency information flow requires not just an examination of the corresponding provisions of intelligence law but also a thorough analysis of criminal procedure law as such (IV.).

# I. The Precaution Paradigm of Security Policy and Changes in the Law

Security policy is to a large degree and in many different ways defined by scientific, technological, political, and social developments.

## A. Technifying the Law

The impact on the security policy from insights into risk and so-called residual risk gained from the natural sciences is paradigmatic. According to the principle of quantum indeterminacy, human knowledge about nature is exposed to ontological limits, because the chain of causation between natural events is not linear and deterministic. This is why any judgment on the course of natural events can only come in the form of probability. Thus, such judgments will always have an inherent residual risk that cannot be predicted.[3] As there is no way to objectively rule out residual risk, so the scientific argument goes, the recommendation for public institutions is to paradigmatically reconsider their actions in keeping with this scientific theory of natural causation.[4]

The incorporation of this approach has considerable consequences for public issues: it has the potential to turn their management into mere risk management.[5] Risk is defined as the scientific unpredictability of factors which the public administration must consider in its decision-making processes. In fact, this approach has already been implemented in the security law on managing technology-related

---

[3] For more details, see *Jaeckel*, Gefahrenabwehrrecht und Risikodogmatik, 85, 219, and 320.

[4] *Jaeckel*, Gefahrenabwehrrecht und Risikodogmatik, 167 and 321 ff.

[5] Compare *Gusy*, Polizei- und Ordnungsrecht, 4.

sources of risk (*technisches Sicherheitsrecht*).[6] In order to cope with these risks, the public administration is supposed to take several measures, including the proactive and precautionary collection of information on potential sources of risk prior to any identifiable danger (*Informationsvorsorge*). The goal is to optimize the administration's ability to act in the event of a specific danger in the future.[7] However, there is an inherent ambiguity between the aim and the means: on the one hand, the precautionary collection of information aims to improve the position of the person in charge who, based on the circumstances of the case at hand, must decide on the probability of a danger in the future. On the other hand, the precautionary collection of information suffers from a lack of reasonable satisfaction: according to the above-mentioned scientific paradigm, this information will never neutralize the subjectivity of judgment of the person in charge. In fact, the knowledge about the decision factors will remain unpredictable not just before and during administrative actions but also in the subsequent retrospective assessment by the judicial authorities. Thus, the standard of the perspective of a reasonable and objective third person is at risk of being abolished.[8] Traditionally, this perspective has been a yardstick for the assessment and adjustment of administrative actions, particularly in police law, in terms of scrutinizing the presence of a specific danger, which triggers the obligation as well as the justification for police action against the causal agent.[9]

## B. Domestic Security as a 'Natural Problem to Solve'

The above-described developments (particularly the factoring in of residual risk and the implementation of precautionary information management) are not just some features specific to administrative law for regulating technical issues.[10] The impacts of the public administration's policy of anticipating dangers, here also called precaution-based policy, are more far-reaching and suggest a shift in paradigms in the entire legal order.[11]

The changes begin at the level of perception of the security situation and its evaluation. The premise is an international order in transition. Globalization and digitization entail both chances and risks such as transnational terrorism or cybercrime. At the same time, anti-globalization appears in the shape of fundamentalist

---

[6] For instance, in the regulation on nuclear power plants or aircraft noise; for more, see *Isensee*, Das Grundrecht auf Sicherheit, 29.

[7] *Jaeckel*, Gefahrenabwehrrecht und Risikodogmatik, 315.

[8] *Jaeckel* Gefahrenabwehrrecht und Risikodogmatik, 147 and 218.

[9] For more, see *Gusy*, Polizei- und Ordnungsrecht, 58 ff.; see also BVerfG NJW 2016, 1784.

[10] For more on this, see *Poscher*, DV 3/2008, 349; *Volkmann*, NVwZ 2009, 217.

[11] See for instance BVerfG NJW 2006, 1946; BVerfG NJW 2008, 1516.

nationalism or religiously motivated violence, jeopardizing the internal security and public order of states. The collapse of nation states ends up paralyzing national economies by corruption or organized crime structures.[12] Cyber risks are an area where overlaps between domestic and foreign security are particularly noticeable.[13] The risks to security arising from these developments are deemed to be unpredictable. They exhibit, so the argument continues, a certain hybridity as they may target all areas of life.[14] Thus, the overall security situation is characterized by risks that are transnational, unpredictable, and diverse.[15]

Furthermore, the well-known security structures at home and abroad increasingly seem to elude a precise assessment by the security authorities. The ability to make an objective assessment is disappearing due to the complexity of security-relevant issues and an instability in the conditions of these issues.[16] The security authorities claim to no longer be able to rely on their knowledge gained from long-standing general experience, as the circumstances and issues are new and the ability to control national borders decreases. All in all, not just security but 'the mere order of things', which until now has been perceived as intact, seems to get out of hand.[17] Public concern is no longer confined to internal and external security, terms typically understood as the national and international conditions for the existence of the state and its constitutional order. Rather, the concerns of the general public about security are increasing and include calls for the protection and preservation of 'the proper order of things' in general. On the whole, law and order policies are becoming more and more acceptable in political, social, and legal discourse.

The response of at-risk societies to their lost sense of security in terms of their place in a globalized world is to demand tighter social and crime control, including across borders. On closer look it appears that the responses to the new perception of the security situation are significantly different from the conventional actions of the public administration and lead to demands for a new architecture of the security policy and the law. As security risks are no longer considered containable or even controllable, a proactive, permanent, and comprehensive approach to security risks is called for.[18] To address these issues requires answers to questions such as:

---

[12] Weißbuch (2016), 28; see also *Sieber*, Der Paradigmenwechsel, 353.

[13] Weißbuch (2016), 37.

[14] Weißbuch (2016), 39.

[15] Weißbuch (2016), 28; for more, see *Poscher*, DV 3/2008, 347; *Zoller*, Rahmenbedingungen nachrichtendienstlicher Informationsgewinnung, 16 ff.; *Daun*, Die deutschen Nachrichtendienste, 56; *Korte*, Informationsgewinnung der Nachrichtendienste, 30.

[16] Weißbuch (2016), 28; see also *Poscher*, DV 3/2008, 348; *Stümper*, Kriminalistik 6/1980, 242.

[17] Compare *Volkmann*, NVwZ 2009, 217.

[18] Compare *Stümper*, Kriminalistik 6/1980, 242 and 244.

– How do people behave?
– What is the extent of potential risks as a result thereof?
– What risks are actually caused and might be averted?
– What are the possible causes or to whom can the risks be attributed?[19]

These seemingly 'simple and harmless' objectives are not just reflections of the basic parameters of the new information-based security doctrine; the mere notion of them will result in a substantial restructuring of security-related government actions. Legally, the theoretical possibility to limit state actions will fall away as all areas of human life, all types of human behaviour, and the individual human being him- or herself are, in their entirety, security-related.[20] The traditional allocation of government actions and the separation of powers into legislative, executive, and judicial branches[21] will disappear, as the overriding question of security requires a holistic approach. The same will apply to the temporal limits on state actions in the form of an identifiable threat (*Bedrohung*), a specific danger (*konkrete Gefahr*), or a reasonable suspicion (*hinreichender Tatverdacht*), because the risks are considered permanent and cannot be completely excluded (due to the inherent residual risk), and because proactive and long-term precaution is considered necessary.[22] A linear and fragmentary response to occurrences, incidents, or events would no longer make sense.[23] To establish a holistic circle of security in compliance with the principle of precaution and in order to close potential gaps, all security authorities must be encouraged to operate pre-emptively, or, to put it in the words of German literature and jurisprudence, in the pre-field of their traditional areas of responsibility.[24] At the same time, proactive investigations must anticipate the need for future measures not only in the jurisdiction of the agency in charge but also of the other agencies to achieve some degree of transferability of the investigation results. As far as the control of criminal conduct is concerned, the primary focus of the new security concept is clearly no longer repression but rather a comprehensive notion of prevention. The former president of the state office of criminal investigation (*Landeskriminalamt*) in Stuttgart, *Stümper*, as early as 1980 framed the underlying principle this way: 'preventing is better than healing, healing is better that securing, securing is better than punishing, punishing is better than a response that

---

[19] Predictive policing seems to be an attempt to answer these questions. However, there are serious doubts about the potential of predictive policing tools. For more, see *Egbert*, European Journal for Security Research 3 (2), 95–114, (2018).

[20] In this regard *Stümper*, Kriminalistik 6/1980, 242 is quite illustrative.

[21] *Isensee*, Das Grundrecht auf Sicherheit, 6 ff.

[22] For more, see *Stümper*, Kriminalistik 6/1980, 242; *Griesbaum*, NStZ 2013, 370.

[23] Referring to this aspect *Volkmann*, NVwZ 2009, 217; see also BVerfG NJW 2008, 829; *Gusy,* Polizei- und Ordnungsrecht, 4.

[24] *Stümper*, Kriminalistik 6/1980, 242; compare BVerfG NJW 2008, 824.

lacks a concept, is indecisive, and dithers back and forth between reaction and non-reaction!'[25]

Even if the government makes no secret of the fact that there is no such thing as absolute security for people in Germany,[26] it seeks in its approach global and flexible answers to security threats and calls for a national security precaution policy (*nationale Sicherheitsvorsorge*), which embraces commerce and industry, science and civil society in addition to the state authorities in order to meet the objective of providing security.[27] As this objective has been declared the joint responsibility of all state institutions (*gesamtstaatliche Aufgabe*)[28], taking precautionary measures for security (*Sicherheitsvorsorge*) requires cooperation on the part of government authorities: for example, in order to be effective in fighting terrorism, the intelligence services and the police must work in close cooperation.[29] In connection with a precaution-based security policy the government emphasizes the significance of a well-functioning early warning system to improve its ability for action and reaction. It is argued that the system must be based on a precise and flexible set of indicators as well as comprehensive analytical capabilities.[30] Further, an upgrade of the corresponding capacities for early and preventive identification of vulnerabilities is key for the government.[31]

## C. Emergence of Precaution-Based Security Legislation

Some aspects of the above-outlined security doctrine also closely related to intelligence and crime control are in one way or another already reflected in more recent German security legislation: for instance, since 1994 the German Federal Intelligence Service (*Bundesnachrichtendienst:* BND) has been tasked with the surveillance of telecommunications with foreign countries. This means that any international telecommunication user in Germany is subject to monitoring by the BND, an agency whose primary responsibility is actually the collection of *foreign* intelligence for the government for the purpose of shaping a national security strategy. This notwithstanding, the agency also conducts strategic monitoring by searching the international telecommunications traffic for certain terms (*Suchbegriffe*) in order to detect early, confront, and address certain serious crimes with

---

[25] *Stümper*, Kriminalistik 6/1980, 243; see also *Volkmann*, JZ 18/2006, 919; *Poscher*, DV 3/2008, 348.

[26] Weißbuch (2016), 59.

[27] Weißbuch (2016), 56.

[28] Weißbuch (2016), 38.

[29] Weißbuch (2016), 34.

[30] Weißbuch (2016), 39.

[31] Weißbuch (2016), 60.

an international connection.[32] As a result of this development, the BND is now a government security agency which—in considerable departure from the principle of separation—is not only in a position of influence over the government's decision-making processes but also over the prevention of specific dangers by means of police law and the administration of justice by criminal law. The consequences of this development for criminal law are substantial; its monopoly on criminal prosecution and control over wrongful conduct appear to be shrinking, since said monitoring does not depend on the presence of a suspicion in respect to at least a criminal attempt.[33] In fact, the Federal Intelligence Service is not at all familiar with such a threshold, which has typically been the justification under criminal law for investigation measures against individuals. Similarly, in 1998 the constitution was amended to enable criminal prosecution authorities to conduct so-called residential surveillance, which may last for quite a long time and aims *inter alia*—in line with the precautionary and anticipatory principle of investigations—at the preventive gathering of information on individuals linked to a criminal organization.[34] As a result, the law appears to suggest, with regard to the latter, a certain inherent 'milieu or relational responsibility'.[35] Thus, by surveilling these individuals even the lower threshold of preventive police law, i.e. the presence of a specific danger, is undercut.[36] The anticipatory objective of said measures is obviously not only to destroy criminal structures but also to secure sufficient evidence for subsequent criminal proceedings against these targets.[37]

After 9/11 and the terrorist attacks in Europe, security legislation continued to be tightened. Legislation on telecommunications provides a further example of security regulations following the precaution paradigm outlined above: in 2008 the legislature introduced an obligation for telecommunication providers to retain, as a precaution, all so-called telecommunication metadata for six months. Data retention by telecommunication providers is designed to enable the security authorities, including the intelligence services and preventive and repressive law enforcement agencies, in their anticipated future actions in a specific case to avert serious dangers to legal interests of constitutional rank, to prevent serious criminal offences, or to prosecute them.[38]

---

[32] For more, see BVerfG NJW 2000, 58 ff.; see also below III.A.1.d) Main Features of Intelligence Investigations and Differences from Preventive and Repressive Police Investigations.

[33] Compare BVerfG NJW 2004, 2217; see also below III.C. Main Concerns.

[34] For more, see BVerfG NJW 2004, 1002 ff.; BVerfG NJW 2016, 1784 ff.

[35] All translations of German texts, legal provisions, or decisions are the authors' own unless indicated otherwise.

[36] On this criterion, see below III.A.2.b) Preventive Policing.

[37] In this regard, see also below III.A.2.e) Main Features of Police Investigations and Differences from Intelligence Investigations.

[38] BVerfG NJW 2010, 839 ff. See also below III.B.2. Precautionary Data Retention.

A non-exhaustive list of other regulations on security measures includes the following:

– preventive electronic profile searches by the police (*Rasterfahndung*),[39]
– automatic number plate recognition (*automatische Kennzeichenerfassung*),[40]
– infiltration into information technology systems by using a so-called state trojan,[41]
– establishment of a joint counter-terrorism database (*Antiterrordatei*).[42]

## II. The Precaution Paradigm of Security Policy – Evaluation under Constitutional Law

The socio-political discourse offers various arguments in defence of the above-described reorientation of the security policy and triggers several different reactions in society. The question whether this reorientation precedes an objectively changed security situation cannot be discussed here. However, people clearly perceive the security situation as increasingly threatening or risky; a growing fear of crime must be noted.[43] At the same time, the precautionary measures of security law, whose numbers have rapidly increased in recent years, especially technical surveillance and information processing measures, have an intimidating effect on people. The assumption is that they cause 'a feeling of being watched', inhibiting the exercise of fundamental rights and freedoms.[44]

The first legal screening which the precautionary paradigm of security law must pass is the constitution.[45] In fact, the German Federal Constitutional Court subjected the question of compatibility of the new security legislation with the constitution to strict scrutiny. The first issue addressed by the Court were the constitutional foundations of the state's duty to provide security.[46] The second issue for purposes

---

[39] BVerfG NJW 2006, 1939 ff. See also below III.B.4.c) Precautionary screening in the pre-field of concrete danger.

[40] BVerfG NJW 2008, 1505 ff. See also below III.B.4.d) Precautionary automatic licence plate recognition in the pre-field of concrete danger.

[41] BVerfG NJW 2008, 822 ff. See also below III.B.3.b) Federal Office for the Protection of the Constitution (BfV).

[42] BVerfG NJW 2013, 1499 ff.; see also below III.B.3.a) Federal Intelligence Service (BND).

[43] *Sieber*, Der Paradigmenwechsel, 353; *Volkmann*, NVwZ 2009, 216.

[44] BVerfG NJW 2008, 1507 ff.; BVerfG NJW 2008, 830; BVerfG NJW 2006, 1944.

[45] For more, see also *Gusy*, Polizei- und Ordnungsrecht, 35 ff.; *Papier*, NJW 2017, 3025 ff.; *Volkmann*, JZ 14/2004, 696 ff.

[46] For a critical assessment, see *Isensee*, Das Grundrecht auf Sicherheit, 1 ff.

of this paper dealt with the constitutional limits of crime control by the intelligence services or by means of intelligence. Both issues are linked, because the stronger the constitutional foundation of the state's duty to provide security is, the fewer the limits.

Regarding the first issue, the Court's corresponding case law addressed three arguments: national security, positive obligations, and negative obligations.[47]

## A. Broader Security Notion

### 1. The Approach of 'Security for the Order of the State'

It is generally accepted that it is the immanent and essential duty of the state to provide and maintain security. The theoretical origins of this notion vary depending on the idea of statehood, the state monopoly on use of force, and the state's function as the guardian of peace and order.[48] In terms of the German constitution, the general obligation and justification to protect the state and the constitution (*Staats- und Verfassungsschutz*) is derived from Article (Art.) 73 no 10 lit b *Grundgesetz* (GG, Basic Law), which describes 'the protection of the free democratic basic order, existence and security of the federation or of a *Land*' as subject to the joint jurisdiction at the federal level and the federal states' (*Länder*) level. Accordingly, all state actors must consider the protection of the state and the constitution the 'overarching responsibility' (*Gesamtaufgabe*) in their respective areas of responsibility and must ensure that this objective is accomplished in the course of their activities.[49] The same assumption applies to the security authorities, regardless of their structural affiliation with the legislature/government (intelligence), the administration (police), or the judiciary (criminal prosecution).[50] This approach may be called 'security for the order of the state'.

As indicated in the arguments related to empirical necessity,[51] the key characteristic of this foundation of national security is that the holistic and integrative work

---

47 For more, see *Gusy,* Polizei- und Ordnungsrecht, 35 ff.

48 See for instance BVerfGE 49, 24, 59, where the Federal Constitutional Court accepts that the state has a legitimate interest in 'self-preservation' (Selbsterhaltungsinteresse des Staates). In its subsequent jurisprudence, however, there is no such reference. On the duty of self-preservation of the state from the perspective of Kant's political philosophy, see *Eberl*/*Niesen*, Kommentar, 274; *Rimoux*, Kants Rechtstheorie vom Weltfrieden, 60.

49 For more, see *Nehm,* NJW 2004, 3292; *Griesbaum*, NStZ 2013, 369; on the so-called concept of 'state protection' (Staatschutz), see also *Graulich*, Sicherheitsrecht des Bundes, 4; critical on this concept *Gusy*, Polizei- und Ordnungsrecht, 2 (it might pave the way to a 'police state').

50 Compare *Gusy*, BND-Gesetz, at 11.

51 See above I.B. Domestic Security as a 'Natural Problem to Solve'.

by the security authorities is considered an indispensable and constitutional duty. At the same time, it is argued that there is one and the same task for all security authorities: the protection of the constitution (*Verfassungsschutz*). Even though the domestic intelligence services carry the general task assigned to them in their name,[52] this task is a 'unified responsibility of the state' ('*einheitliche Staatsaufgabe*') in the sense that it is the duty of all state authorities to protect the constitution. All security authorities contribute to 'the protection of the free democratic basic order, existence and security of the federation or of a *Land*', as prescribed in the constitution.[53] Thus, the only meaningful way in which the authorities can carry out the 'concerted responsibility of the state' is by cooperation. This means that cooperation between the intelligence services and the criminal prosecution authorities in well-established overlap areas is not exclusive to specific crimes against the security of the state (*Staatsschutzdelikte*).[54] The same cooperation is required with regard to all crimes committed for anti-constitutional political purposes (*politisch motivierte Straftaten*: the so-called politically motivated criminal offences).[55] With cooperation as the guiding principle, any strict separation of the agencies runs counter to the cooperation requirement as this would create an obstacle to performing their duty under the law. Still, the law may assign special jurisdiction to individual authorities. The lawmaker may consider it necessary to provide both for an appropriate design of the security architecture and for limitations on an excessive use of power by the authorities.[56] The limits of any potential separation of the authorities are therefore not set by the constitution independently; rather, this is the prerogative of parliament.[57] In the final analysis, the answer to the main question of how to regulate intelligence and crime control will usually be left to the wisdom of the legislature. Obviously, this approach, which favours redesigning the architecture of the security authorities for reasons of effectiveness, is bound not to maintain traditional distinctions between intelligence, police, and criminal prosecution investigations based on gradual thresholds and different *modi operandi*[58] and to advocate fundamental shifts in the security structure.

---

[52] For more, see below III.A.1.c) Federal Office for the Protection of the Constitution (BfV).

[53] *Nehm*, NJW 2004, 3292.

[54] For more, see below III.A.2.d) Overlaps between Preventive and Repressive Police Investigations and IV.B.2.b) Unsolicited information transfer.

[55] For more, see below III.A.1.c) Federal Office for the Protection of the Constitution (BfV).

[56] *Nehm*, NJW 2004, 3295.

[57] *Nehm*, NJW 2004, 3292.

[58] For more, see below III.A.1.d) Main Features of Intelligence Investigations and Differences from Preventive and Repressive Police Investigations.

## 2. The Approach of 'Freedom only within Security'

The state's duty to provide security is also based on the positive obligations of the state to protect the basic rights of its people (*Schutzpflichten*). In fact, the function of basic rights as an object of protection has already been acknowledged.[59] What is new is the expansion of the positive obligations of the state to include a subjective and enforceable basic right to security (*subjektiv-einklagbares Grundrecht auf Sicherheit*). It is striking that the proponents of this position base the state's duty to provide security on this very right, in conjunction with the principle of statehood and the state monopoly on use of force.[60] Their argument is in line with the Hobbesian vision that the sole legitimacy and the primary function of the state are derived from the obligation to protect its people against assaults (*Übergriffe*) by others.[61] This crucial rationale, so the argument continues, is entirely overlooked where security is merely understood as the protection of state institutions and the protection of a legal order used by the people to resolve disputes among themselves.[62] According to this approach, the state fails to fully meet its positive obligations if it simply provides institutional guarantees. More specifically, the positive accomplishments of the state are not exhausted by introducing and establishing a legislative framework that would not only leave the enjoyment of security by individuals to the discretion of the legislature, but the entitlement to security would also be downgraded to a simple sub-constitutional right (*einfachgesetzliches Recht*): in the event of a conflict between the requirements of security and freedom of the others security would suffer from its conceptual handicap and be forced to give way to freedom.[63] However, given a constitutional rank of the positive obligation of the state to prevent the assault by others, the presumed antinomy between freedom and security would arguably come to an end, as they would be two equal, constitutionally based guarantees, with only tension remaining between them.[64] Moreover, so the argument continues, there is no security if the state merely refrains to arbitrarily or unduly interfere with the basic rights and freedoms of the people or if it merely regulates and ensures legal security. Furthermore, it is suggested that security as an accomplishment is first and foremost not a legislative but an administrative issue, namely the result of law enforcement activities, which

---

[59] BVerfGE 49, 24, 53 ff.

[60] *Isensee*, Das Grundrecht auf Sicherheit, 2 and 24; see also *Hermes*, Der Staat 24/1985, 119.

[61] *Isensee*, Das Grundrecht auf Sicherheit, 11 and 17; see also *Hermes*, Der Staat 24/1985, 118.

[62] For more on Kant's philosophy-based concept of legal security, see *Rimoux*, Kants Rechtstheorie vom Weltfrieden, 60; *Geismann*, ZphF 37/1983, 364.

[63] *Isensee*, Das Grundrecht auf Sicherheit, 2.

[64] *Isensee*, Das Grundrecht auf Sicherheit, 21.

establish and maintain the status quo.[65] In fact, this security is immediately jeopardized by people who violate their own obligation to keep the peace (*Friedenspflicht*). The renunciation of their own use of force (*Eigenmacht*) and their self-subordination to the state order are at the very core of the obligation to keep the peace.[66] But it would be a contradiction if the people affected did not have a subjective and enforceable right to security where the state fails to protect them against breaches of the peace by others.[67] The basic rights are not only negative obligations of the state or the legal position of the 'disturber' (*Störer*) but also of the victims.[68]

Still, the concept of a right to security has a serious problem: it is not possible to define the specific measures a state must take to protect its people. The right to security needs to be regulated, formulated, and detailed by the legislature,[69] which has a certain margin of discretion in specifying the means to be used to provide security.[70] Thus, the concept of the right to security allows the state to determine, within the limits of its political responsibility, the security concepts considered to be appropriate and necessary. However, this discretion is also subject to constitutional scrutiny, including the right to security.[71] Moreover, this approach accepts that the constitutional obligations of the state neither provide nor require total security. Every society must live with a certain amount of inevitable residual risks.[72] Furthermore, a right to security 'mediated' by statutory law is unavoidable due to the principle that, under the constitution, administrative acts and interventions in basic rights must be regulated by statutory law (*Gesetzesvorbehalt*).[73] This also justifies to define thresholds, which determine when law enforcement is obligated and justified to intervene for the prevention of danger. As the factual and legal conditions by which the thresholds are defined also impact the basic rights and freedoms of the people affected by them, the legislature may consider certain factors when balancing the legal interests in keeping with the principle of proportionality: factors such as the level of danger, the intensity of the measure in question, the abstract importance of legal interests in question (as target of security measures or as at risk), the probability that an anticipated harm will occur, the responsibility of the targeted person, etc.[74] Also, the public administration has a certain margin of

---

65 *Isensee*, Das Grundrecht auf Sicherheit, 22 and 41.
66 *Isensee*, Das Grundrecht auf Sicherheit, 23.
67 *Isensee*, Das Grundrecht auf Sicherheit, 28.
68 *Isensee*, Das Grundrecht auf Sicherheit, 32.
69 *Isensee*, Das Grundrecht auf Sicherheit, 37.
70 *Isensee*, Das Grundrecht auf Sicherheit, 38.
71 *Isensee*, Das Grundrecht auf Sicherheit, 40.
72 *Isensee*, Das Grundrecht auf Sicherheit, 41.
73 *Isensee*, Das Grundrecht auf Sicherheit, 42; see also *Hermes*, Der Staat 24/1985, 118.
74 *Isensee*, Das Grundrecht auf Sicherheit, 37.

discretion to decide whether or not to intervene and how to intervene in the individual case.[75]

In the final analysis, the above-outlined concept of a right to security remains within the conventional limits of conferring security obligations on the public administration. It is acknowledged that law enforcement is not obligated to take a specific measure in the individual case. Nevertheless, the constitutional foundation of the right to security has clear implications: first, it establishes an entitlement for the people to demand legislative action and a correct use of the margin of discretion by law enforcement in the specific case.[76] Second, the right to security constitutionally justifies the security measures of law enforcement, which ultimately benefit individuals. The fact that the right to security is not a mere reflection of fulfilling a general duty to provide security but rather a subjective and enforceable right is also manifested in the fact that people are also entitled to resort to their right to self-redress (*Selbsthilferecht*) if the state fails to meet its obligation.[77]

Critics claim that the above-outlined right to security is a rather weak 'basic right' in that it cannot compel the state to take a specific action and, as such, is simply meaningless.[78] Instead it is suggested that the entire project to establish a basic right to security is a political venture.[79] The political component of this argument can also be seen in the reference to the added obligation for the state to provide education promoting security and to avoid societal policies detrimental to security.[80]

Regardless of this theoretical criticism, the concept of a right to security provides some basic ideas which compel the state to take precautionary action not only in the area of technology-related risks but also for the very enjoyment of basic rights and freedoms. In fact, it postulates a guarantor position (*Garantenstellung*) for the state when acts of the state, such as the approval of a nuclear power plant, have a double effect (*Doppelwirkung*) in the sense that the approval impacts not just the operator but the residents in the neighbourhood as well.[81] The double-effect argument is based on a simple notion: by approving one condition, the administration may also create a source of danger for others.[82] While the state's legitimate approval is principally to the benefit of the public interest, the state must at the same time, in the interests of the residents, take precautionary action against potential risks. Finally, legislative action in terms of security is subject to the principle of effec-

---

75 *Isensee*, Das Grundrecht auf Sicherheit, 53.

76 *Isensee*, Das Grundrecht auf Sicherheit, 50 ff.; *Hermes*, Der Staat 24/1985, 118.

77 *Isensee*, Das Grundrecht auf Sicherheit, 56 ff.

78 *Hermes*, Der Staat 24/1985, 121.

79 *Hermes*, Der Staat 24/1985, 121.

80 *Isensee*, Das Grundrecht auf Sicherheit, 39 ff.

81 *Isensee*, Das Grundrecht auf Sicherheit, 29.

82 *Isensee*, Das Grundrecht auf Sicherheit, 34.

tiveness. It is argued that 'new kinds of security necessities' have emerged,[83] which the conventional measures of the police and criminal law can no longer address.[84]

This line of argument allows a broader analogy: the entire spectrum of exercising basic rights and freedoms may be seen as fraught with potential risks that are permitted and in the public interest, even though the state as 'organizer' is compelled to take precautionary measures to protect other interests. In other words, the risks attached to the individual use of basic rights arise from the scope of action that the state itself accords to others. Thus, it can be argued that the state assumes the position of a general guarantor. As such it would be compelled first of all to control people in the exercise of their basic rights and freedoms. Second, it would be required to protect those who are restricted in their scope of action as a result of risks emerging from the use of basic rights and freedoms by others. This approach may be called 'freedom only within security'. Remarkably, the requirements of such an approach fit the precaution-based security paradigm which, as highlighted above, aims to collect the following information or to meet the following objectives: how do people behave, what is the extent of potential risks as a result thereof, what risks are actually caused and might be averted, and what are the possible causes to which the risks can be attributed?[85]

### 3. Position of the German Federal Constitutional Court

The position of the German Federal Constitutional Court on statehood or the right to security is nuanced. The Court accepts that the state's pre-eminent feature is its purpose and power to maintain peace and order (*Staat als Friedens- und Ordnungsmacht*)[86] and thus rejects a state's duty to provide security predicated on the notion of the state as an end in itself.[87] Aside from security as purpose of the state (*Sicherheit als Staatszweck*), in terms of the argument of a basic right to security, the Court seems to acknowledge that the state's duty to provide security is not limited to safeguarding the legal order in an impersonal and formal sense. The Court explicitly states that the state's duty to provide security also includes the safety of the people (*Sicherheit der Bevölkerung*). As a consequence, the Court incorporates in its judgment more subjective notions of security, such as the prominent argument of an 'increased fear of crime'. However, this does not imply that the Court

---

[83] *Isensee*, Das Grundrecht auf Sicherheit, 17.

[84] *Isensee*, Das Grundrecht auf Sicherheit, 33.

[85] For more, see above I.B. Domestic Security as a 'Natural Problem to Solve'.

[86] BVerfGE 49, 24, 53; BVerfG NJW 2006, 1942; see also *Nehm*, NJW 2004, 3292; *Griesbaum*, NStZ 2013, 369; for more on the philosophical foundations of the justification of the state as protector of legal security in Kant's political philosophy, see *Rimoux*, Kants Rechtstheorie vom Weltfrieden, 60.

[87] *Rimoux*, Kants Rechtstheorie vom Weltfrieden, 60.

recognizes a subjective and enforceable basic right to security. Rather, the safety of the people mirrors the state's obligation to provide security. At the same time, the Court derives from the objective function of basic rights and freedoms as organizing principles (*Grundrechte als Ordnungsprinzipien*) an obligation[88] of the state to ensure and provide its citizens with security in terms of their life, limb, and freedom.[89] As said, the state's duty to provide security is not based on a subjective and enforceable basic right with regard to these individual interests but on the objective value of these interests for the constitutional order.[90] Moreover, the Court acknowledges that the state's obligation, say, to counter terrorist efforts intentionally targeting the lives of innocent people must be met effectively.[91] Nevertheless, the constitution requires the legislature to strike a reasonable balance between freedom and security. This requirement not only excludes pursuing 'absolute security', which could hardly be achieved and respective attempts would in any case only come at the price of abolishing freedom. The pursuit of the highest possible level of security, under the constitution, is only feasible in the absence of disproportionate infringements on basic rights and freedoms by the security authorities. For the Court, the latter prohibition sets the limit for the state's obligation to protect the individual.[92]

In other words, security as purpose of the state (*Staatszweck*) must be provided within the limits of the rule of law. In order to accomplish this purpose in light of the contemporary threats and risks emerging from terrorism, organized crime, extremism, or the use of information technologies, the Court explicitly states that the legislature is allowed to redefine the responsibilities of the security authorities and, in particular, to authorize them to use new investigative measures no longer based on the conventional definitions of threat (*Bedrohung*), danger (*Gefahr*), or suspicion (*Verdacht*).[93] However, in reconfiguring the security framework, the legislature is not allowed to fundamentally change the balance between security and freedom.[94] Remarkably, the Court arrives at an opposite conclusion regarding the state's constitutional obligation to provide security in that it does not prioritize security as the purpose of the state and states that the constitution prescribes, as a matter of principle, a separation of the responsibilities, powers, and information of the intelligence, police, and criminal prosecution authorities. Despite the importance of this constitutional support, the constitutional reach of this principle of

---

88 For more on this notion, see *Isensee*, Das Grundrecht auf Sicherheit, 27.

89 BVerfGE 49, 24, 53; BVerfG NJW 2006, 1942.

90 BVerfG NJW 2004, 1000 ff.

91 BVerfG NJW 2006, 1945.

92 Ibid.

93 See examples below III.B.1. A General Overview: Restructuring the Security Architecture.

94 BVerfG NJW 2008, 1515; BVerfG NJW 2006, 1946.

separation has not yet been specified and should not be overestimated at first glance. Even so, it allows overlaps and parallels between the responsibilities of the intelligence, police, and criminal prosecution authorities as long as there is no 'unconstitutional intermingling'.[95] Moreover, the Court does not *per se* prohibit the authorities from being assigned to operate in the pre-fields of their customary areas of responsibility[96] or the police and criminal prosecution authorities from being empowered to use methods of intelligence[97] or to share information.[98] Rather, it sets some limits. In fact, the exact scope of crime control by the intelligence services or by using the intelligence measures of the police and criminal prosecution authorities can only be appreciated if the corresponding provisions of these areas of the law are explored, as will be detailed below.[99]

Furthermore, the Court abstains from requiring the legislature or administration to apply a certain policy or take certain measures. It justifies this by noting that it is the prerogative of a democratically elected government to decide on the security policy and to choose certain security measures over others.[100] It requires state authorities to take only those security measures that do not fall below certain minimum standards. Again, the Court proves to be rather cautious in its judgment, as the pro-security approaches disregard the core issue of security regulations, namely the question of the degree to which state authorities are allowed to interfere with basic rights and freedoms. The argument of the positive obligation of state, *a fortiori* in the form of a subjective basic right to security, has considerable potential to subvert the application of the principle of proportionality and to justify disproportionate interference by reference to the state's obligation to protect. In fact, as *Gusy* highlights, 'a state that would be obliged to protect everything must know everything, control everything, be able and allowed to do everything.'[101] In that case, the proportionality test would not result in any substantive limits and could only prohibit unsuitable or needless security measures.[102]

Following up on these critics, the third model of the foundations of security law emphasizes the primary function of basic rights and freedoms as negative (subjective) obligations of the state that must be equally respected within the framework of

---

95 BVerfG NJW 2000, 60; BVerfG NJW 2004, 2214.

96 See below III.B.3.a) Federal Intelligence Service (BND).

97 See below III.B.4. At the Level of the Police.

98 See below IV.B. Transfer and Use of Intelligence Information at Investigation Stage.

99 Ibid.

100 According to the jurisdiction of the Court, the government will inform the public about the content and scope of a security regulation, which will then have the opportunity to influence the representatives, BVerfG NJW 2008, 1509; BVerfG NJW 2008, 829; see also BVerfG NJW 2004, 1009; *Isensee*, Das Grundrecht auf Sicherheit, at 38 ff.

101 *Gusy*, Polizei- und Ordnungsrecht, 36.

102 BVerfG NJW 2006, 1945.

security law. As a result, this model insists on a fair balance between freedom and security and only allows regulations capable of passing the proportionality test. This approach may be called 'security only within freedom'.

## B. Differentiated Security Notion

### 1. The approach of 'Security only within Freedom'

A quick glance at the case law of the Federal Constitutional Court shows that it does in fact not fail to address the fundamental importance of freedom in the process of designing the new security architecture. The Court not only takes note of the necessity for reorienting the security policy in light of contemporary risks and threats. It is also explicit in pointing out that the threat to exercising the constitutionally guaranteed basic rights and freedoms has grown considerably over the past several decades. On the one hand, the Court accepts that the use of modern telecommunication technologies and computer systems involves specific security risks, even though modern technology improves the security authorities' investigative effectiveness.[103] On the other hand, the use of these technologies has become an integral part of an individual's daily and social life and, consequently, a space for exercising one's basic rights and freedoms. As a result, the authorities are in a position to reveal the personality of affected persons to an extent not at all possible in the past.[104] In other words, the developments constituting a threat to freedom such as interferences with the integrity of the home, telecommunications, and computer systems are first a result of technological innovations creating enormous capacities for collecting and processing personal data in different ways.[105] In fact, measures of security law, which in recent decades have increasingly intensified, involve considerable risks for individuals while they enjoy their basic rights and freedoms. The existing possibility to proactively and comprehensively profile individuals in terms of their behaviour, communications, or movements has an intimidating effect on people, regardless of the legitimate purposes for doing so.[106] Moreover, as the Court highlights, any interference with individual self-determination constitutes an impairment not only of an individual's personal interests but also of the interests of the general public, as self-determination is essential for the ability of citizens to act

---

[103] BVerfG NJW 2004, 1009; BVerfG NJW 2006, 981; BVerfG NJW 2008, 828 ff. (the use of the so-called 'state trojan' by the Intelligence Service of North Rhine-Westphalia); see also the landmark decision of the Federal Constitutional Court BVerfGE 65, 1, 41 ff.

[104] On the use of the so-called 'state trojan', see for instance BVerfG NJW 2008, 828 ff.

[105] On this, see BVerfG NJW 2004, 1000.

[106] BVerfG NJW 2008, 1507 ff. (by the automatic licence plate recognition system used by the preventive police); BVerfG NJW 2008, 824 ff. (by the so-called 'state trojan' used by the domestic intelligence service).

and to participate, which is the foundation on which the idea of a free and democratic society is based.[107]

In consideration of the risks arising from measures of security law, the Court requests to reduce them to an 'acceptable' level in accordance with the rule of law principle while balancing freedom and security.[108] Hence, the function of basic rights and freedoms as negative obligations and the proportionality test are the key determinants of the Court's case law. The Court emphasizes that the basic rights and freedoms are not merely objective organizing principles (*Grundrechte als Ordnungsprinzipien*), which the state must consider in establishing the conceptional limits of its security policy. The basic rights and freedoms are also guarantees for the subjective position of their holders, they account for the negative obligations of the state (*Grundrechte als Abwehrrechte*),[109] and to provide them is the equivalent of providing public security.[110] Thus, the granting of basic rights and freedoms confirms Germany's identity as a society with a free democratic basic order.[111]

The development of the above-outlined jurisprudence emphasizing the negative obligations of the state in the context of security may be traced back to 1970s. For the Court, restrictions on basic rights and freedoms of individuals by actions of the intelligence services—in the case at issue it was the so-called strategic monitoring of telecommunication traffic with abroad—raise the question of a no less pivotal landmark decision under the constitution, namely on the extent to which the protection of the constitution may justify interference with basic rights and freedoms.[112] When the Court subsequently, in 1983, deduced in its famous census judgment (*Volkszählungsurteil*) a right to informational self-determination[113] from the guarantee of human dignity (Art. 1 I GG) and the right to respect the personality (Art. 2 I GG), it was immediately clear that the entire spectrum of information gathering by the security services was going to be subject to constitutional scrutiny, and not just serious interferences with the privacy of correspondence, mail, and telecommunication (Art. 10 GG). In fact, the security agencies had already been collecting personal data in the pre-field of any identifiable threats, specific danger, or reasonable suspicion in order to prepare for the precautionary prevention of danger to public and individual legal interests (*Gefahrenabwehrvorsorge*) or the precaution-

---

107 BVerfG NJW 2006, 979.

108 BVerfG NJW 2004, 2216.

109 Critical on this, *Isensee*, Das Grundrecht auf Sicherheit, 31 ff.

110 BVerfG NJW 2006 1942.

111 BVerfG NJW 2004, 1013.

112 BVerfG NJW 1971, 277; emphasizing the function of basic rights and freedoms as negative obligations of the state (Grundrechte als Abwehrrechte) in security law, see also BVerfG NJW 2004, 1000 ff.

113 BVerfGE 65, 1, 41 ff.

ary preparation of criminal proceedings (*Strafverfolgungsvorsorge*).[114] Unlike other typically intrusive or compulsive measures, the respective observation and information gathering activities in the pre-fields of traditional thresholds of intelligence, police, or criminal prosecution laws were at that time not considered significant in terms of basic rights and freedoms. Only after the right to informational self-determination had been established, was the gathering of pre-field information by the security authorities considered an infringement on a constitutional right that could only be justified by a parliamentary law.[115] For the sake of the right to informational self-determination, the Court started to consider any further use of personal data collected for purposes other than the primary one as a new infringement of this right. As a result, the transfer of information between the intelligence services, police, and criminal prosecution authorities became an important constitutional question. In fact, ever since, the entire spectrum of information transfer between the security authorities has become the most prominent aspect of the separation question.[116]

With its jurisprudence outlined above, which basically emphasizes the negative obligations of the state and requires the separation of security-related tasks, the German Federal Constitutional Court placed the entire issue of internal security in a constitutional framework. The adoption of new security policies and the restructuring of the security architecture are not mere issues of governmental or administrative decision-making but rather profoundly constitutional questions. The government, by its policy of including the involvement of the intelligence services, or the administration, by its law enforcement agencies including the police, must not decide on them based on reasons of expediency. In the words of the Court, a decision on the limits of the freedom of citizens must not be left unilaterally at the discretion of the administration.[117] The administration's scope of action must be determined by parliamentary law, which will not only limit it but will also ensure the legitimacy of the executive's action and protect the freedom of the people. The implementation of security policies requires in the first place the enactment of a parliamentary law that satisfies the principles of clarity and certainty.[118] Second, the policies must pass the Court's proportionality test whenever basic rights and freedoms are infringed for security purposes.[119]

---

[114] BVerfG NJW 2004, 2216.

[115] BVerfG NJW 2004, 2216.

[116] For more details, see below IV.B. Transfer and Use of Intelligence Information at the Investigation Stage.

[117] BVerfG NJW 2004, 2216.

[118] BVerfG NJW 2005, 2610.

[119] On the constitutionality of the automatic licence plate recognition system by the police for purposes of preventive police investigations, see BVerfG NJW 2008, 1507 ff.

In view of the foregoing, it is obvious that the German Federal Constitutional Court did not entirely approve of the above-outlined precautionary and anticipatory holistic security doctrine.[120] Legally, security policies are still only possible in Germany if they are well differentiated.[121] The Court appears to be convinced that differentiated approaches in security law are necessary as the only way to strike a balance between freedom and security, taking a variety of factors into account. The constitutional requirements also provide the main boundaries for the legislature when it tasks the intelligence services with crime control or equips the police and criminal prosecution authorities with intelligence measures.

A closer look at the Court's subsequent jurisprudence on security law reveals that the constitutionally required balance is based on two main pillars: (1) regarding the security authorities, the scope of actions of the security services must be limited, in particular considering the protection of affected basic rights and freedoms and the principle of proportionality, and (2) the new security architecture is subject to certain structural requirements mainly associated with further consequences of the proportionality test. In some cases, the proportionality test may result in prohibiting the security authorities from pursuing certain aims or resorting to certain methods, or from utilizing certain information at all. These prohibitions are constitutional prohibitions for the security authorities.[122] Similarly, the proportionality test requires a strict balancing between the public and individual interests at issue. This is first and foremost the responsibility of the legislature and requires, at a minimum, a reasonable, clear-cut, and unambiguous definition of the reason for and the purpose and limits of basic rights interventions for each of the three security-related branches.[123]

In the following we will provide (a) a general overview on how the proportionality test works in the context of security law, and (b) and how the restructuring of the security architecture challenges the proportionality test. This will prepare for the next subsection, which will cover intelligence law, police law, and criminal prosecution law in more detail (III.). The question of separation in terms of information sharing, in particular the introduction of intelligence into criminal proceedings, will be explored in a separate section (IV.).

---

120 See above I.C. Emergence of Precaution-Based Security Legislation.

121 For a differentiated risk prevention model, see *Gusy*, Polizei- und Ordnungsrecht, 37.

122 For more, see BVerfG NJW 2006, 1945 ff.

123 BVerfG NJW 2008, 1509 ff.; BVerfG NJW 2008, 831.

## 2. The Proportionality Test in Security Law

### *a) General overview*

To determine proportionality in the balance between the interests of individuals and those of the general public requires to establish, on the side of individual interests, which, how many, under what conditions, and to what degree basic rights holders are subject to restrictions. On the side of public interests, the decisive factor is the weighing of aims and issues: how significant is the legal interest to be protected by the measures in question and what is the probability of actual harm to the legal interest in question?[124] The failure to provide for these factors or an imprecise wording of these factors not only carries the risk of disproportionate restrictions on basic rights and freedoms in the individual case but may also result in the unconstitutionality of the law in question for failure to comply with the clarity principle.[125]

Whereas some of these proportionality test-factors are normative and require corresponding consideration for the specific circumstances of a security measure (i.e. the level of restrictions on basic rights and the significance of the public legal interest), others are rather empirical (i.e. conditions, target of measures, risk of harm). The latter are considered collectively by stipulating thresholds for certain activities by the security authorities. Additionally, the thresholds need to be specified in terms of the factual basis and degree of probability regarding the presence of the aforementioned empirical factors. As the thresholds more or less define the time when the security authorities are justified or obligated to interfere with basic rights and freedoms, they are crucial in the constitutional balancing of freedom and security as well as for the functioning of the security authorities. In specific cases, the authorities are called upon a so-called probability judgment (*Wahrscheinlichkeitsurteil*) in accordance with the statutory thresholds in light of the circumstances of a case. One example illustrating the implementation of these proportionality requirements in security law is the traditional threshold applied in preventive policing, which is the presence of a *concrete danger* for a legal interest under protection of police law.[126] This threshold amounts to the question whether it is reasonably likely that, in the individual case, in the absence of police intervention, a certain person may cause harm to the protected legal interest in the near future. Thus, the probability judgment involves the temporal proximity of a risk that might turn into harm and the reference to an individual as originator. As such, the threshold always consists in an assessment of these three components: a specific case, said temporal

---

124 BVerfG NJW 2008, 1515; BVerfG NJW 2006, 1946; BVerfG NJW 2000, 63.

125 BVerfG NJW 2005, 2610.

126 On these legal interests, see below III.A.2.b) Preventive Policing.

proximity, and the designation of a responsible causal agent.[127] As the latter component implies, it is an important question for purposes of the proportionality test whether the person to be affected by a security measure has given rise to the public intervention as a result of his or her behaviour. Preventive police law reflects the proportionality factor in that police investigations are generally restricted to investigations against the so-called 'disturber' (*Störer*) as the person responsible in terms of police law.[128]

With regard to the quality of the factual basis on which the conclusion and assumptions of the probability judgment will be based, security legislation usually uses the notion of facts (*Tatsachen*) or factual indications (*tatsächliche Anhaltspunkte*). The latter is generally regarded as less stringent than the former.[129] However, even the constitutional requirement of factual indications means that presumptions or general experiences by themselves are not sufficient to form the factual basis for an interference with basic rights and freedoms.[130] Rather, individual circumstances (*konkrete Umstände*) must be identified that can support the required degree of probability.[131] This excludes diffuse and less substantial factual circumstances that are difficult to grasp or may be interpreted in different ways.[132] In each case, the circumstances must allow drawing a well-founded conclusion with regard to the subject matter and the required degree of probability. Purely subjective assessments by the authorities fraught with considerable uncertainties and resulting in random investigation measures ('*ins Blaue hinein*') against the individual are constitutionally prohibited.[133]

The German Constitutional Court attaches considerable importance to the degree of probability and the quality of its factual basis. It establishes a correlation between these two factors and the weight of the harm anticipated or done to the

---

[127] BVerfG NJW 2010, 831 ff.; *Roggan*, NJW 2009, 257; for more, see below III.A.2.b) Preventive Policing.

[128] For more, see below III.A.2.b) Preventive Policing.

[129] BVerfG NJW 2004, 2218.

[130] BVerfG NJW 2000, 67 (strategic monitoring by the Federal Intelligence Service); BVerfG NJW 2006, 1947 (police screenings for preventive purposes); BVerfG NJW 2004, 2218 (preventive wiretapping by the Federal Customs Criminal Police Office); BVerfG NJW 2005, 2608 (precautionary wiretapping by the police); BVerfG NJW 2008, 831 (use of the so-called 'state-trojan' by the intelligence service of North Rhine-Westphalia).

[131] BVerfG NJW 1971, 278 (strategic monitoring by the intelligence services); BVerfG NJW 2000, 67; BVerfG NJW 2008, 1516 (use of the automatic licence plate recognition system by the police for preventive purposes); see also BVerfG NJW 2005, 2607 ff.; BVerfG NJW 2016, 1784 (use of surveillance measures by the Federal Criminal Police Office for preventive purposes).

[132] BVerfG NJW 2004, 2217; BVerfG NJW 2005, 2607 ff.; BVerfG NJW 2008, 831; BVerfG NJW 2016, 1785.

[133] BVerfG NJW 2010, 845; BVerfG NJW 2008, 1515; BVerfG NJW 2008, 831; BVerfG NJW 2006, 1946.

legal interest concerned and the weight of restrictions on the basic rights and freedoms of affected persons. The Court emphasizes that, as a rule, even if the public interest at issue is very important, the proportionality test requires that the anticipated future harm be sufficiently probable.[134] Moreover, certain highly intrusive infringements on basic rights and freedoms may only be justified for the protection of certain public legal interests, provided there is a minimum level of qualified suspicion and danger.[135] A serious interference with basic rights may already be disproportionate if the statutory weight of the reason to interfere (type and degree of suspicion or danger) is insufficient.[136] Furthermore, the Court provides the following guideline for balancing: the more substantial the infringement of the legal interest that is threatened or has already occurred and the less substantial the infringement of basic rights at issue, the lesser the probability needs to be which indicates that an infringement is anticipated or has already occurred, and the less substantiated, if necessary, the facts underlying the suspicion may be.[137] *Vice versa*, the less substantial the legal interest at risk, the higher the requirements for prognostic reliability (*Prognosesicherheit*) both in terms of the level and the intensity of risk.[138]

### *b) Separation of the security functions in light of proportionality*

In balancing freedom and security in light of the above-outlined factors, the legislature has the possibility to adjust the conditions of investigative measures according to the specific characteristics of the security-related task that needs to be accomplished: for instance, it is an established standard of the law that, for repressive criminal prosecution, in order to initiate a criminal investigation against a person, the required minimum is the presence of a suspicion of a criminal attempt (so-called 'initial suspicion': *Anfangsverdacht*). As mentioned above, a preventive police investigation typically requires the presence of a specific danger (*konkrete Gefahr*) in terms of a legal interest protected under police law.[139] However, neither threshold—the suspicion of a crime and a specific danger—matches the way in which the intelligence services conduct investigations, as they are responsible for recognizing potential threats or efforts in the pre-field of an initial suspicion and of specific dangers. The Federal Constitutional Court considers this differentiated management of thresholds justified because the legal interests and legal outcomes

---

134 BVerfG NJW 2008, 831 (use of the so-called 'state-trojan' by the intelligence service of North Rhine-Westphalia); BVerfG NJW 2008, 1515 (use of the automatic licence plate recognition system by the police for preventive purposes); BVerfG NJW 2006, 1946 (police screening for preventive purposes).

135 BVerfG NJW 2008, 831; BVerfG NJW 2008, 1515; BVerfG NJW 2006, 1946.

136 BVerfG NJW 2008, 831.

137 BVerfG NJW 2008, 1515; BVerfG NJW 2006, 1946.

138 BVerfG NJW 2005, 2610.

139 BVerfG NJW 2004, 2216.

protected or produced by intelligence are different from those in preventive and repressive police investigations.[140] To briefly illustrate the rationale behind this justification:[141] the strategic monitoring of international telecommunication traffic by the German Foreign Intelligence Service (*Bundesnachrichtendienst:* BND) aims to collect information on certain threats relevant to foreign and to security policy. This information gathering is characterized not only by the lack of a reference to a specific person but also by its limited use for purposes of government consultation. This purpose provides the justification for the difference in conditions for strategic monitoring compared to similar measures under preventive police or criminal procedure law.[142] Most importantly, the German Federal Constitutional Court emphasizes that information sharing between the intelligence services and the police authorities is prohibited as a matter of principle. Departures from this principle are permitted only by exception.[143]

As a result, by defining the material, temporal, and personal conditions of involvement and the specific investigation measures of intelligence services on the one hand and preventive or repressive police authorities on the other, the legislature establishes the respective thresholds for intervention (*Eingriffsschwellen*). In doing so, it establishes not only external boundaries for security governance but also internal boundaries between intelligence, police, and criminal prosecution.

The separation of security functions outlined above and based, *inter alia*, on the proportionality principle is challenged by measures of the new security law that involve a considerable restructuring of the conventional security architecture. As already mentioned, the Federal Constitutional Court accepts that in order to provide security in light of the contemporary threats and risks such as those emerging from terrorism or extremism some amount of restructuring of the security architecture may be required.[144] The departures from conventional measures occurred at many levels and in a variety of ways: the first question raised by almost all respective regulations is whether the new responsibilities, powers, legal concepts, or offences are still within the boundaries of or supported by the dogmatic foundations of intelligence law, police law, and criminal law. The second issue questions the genuine functions of intelligence law, police law, and criminal law and whether some functions of the respective areas have now been assumed or undermined by other areas.

---

[140] BVerfG NJW 2000, 63.

[141] For more, see below III.A.2.e) Main Features of Police Investigations and Differences from Intelligence Investigations.

[142] BVerfG NJW 2000, 63; see also BVerfG NJW 1971, 280.

[143] BVerfG NJW 2013, 1505; compare BVerfG NJW 2000, 65.

[144] BVerfG NJW 2006, 1946; see also BVerfG NJW 2008, 824; BVerfG NJW 2008, 1515.

In order to illustrate the key questions paraphrased above in light of the respective constitutional boundaries of proportionality, we will first describe, by drawing on selected issues, the conventional concepts of German intelligence law, police law, and criminal prosecution law, and then their re-conceptualization. Second, we will attempt to show how the Federal Constitutional Court readjusted the proportionality requirements and approved a number of changes and also rejected some for being insufficiently proportionate to the protection of basic rights and freedoms.

# III. Intelligence, Police, and Criminal Prosecution

## A. Conventional Concept

As can be inferred from the discussions above, security-related responsibilities in Germany are divided between three functional categories: intelligence, prevention, and repression. The organizational structure of the authorities established by statute to perform these duties is also based on the distribution of security-related tasks.[145] Further, the principle of separation in German security law rests on the federal structure of the state enshrined in the constitution and the protection of basic rights and freedoms, in particular the proportionality requirement as shown above.[146]

### 1. Intelligence Services

#### *a) Structure*

The objective of intelligence services in general is to contribute to the development of the domestic and foreign security policy of the state. German intelligence services are regulated and organized according to the legislative competences at the federal and at the *Länder* (federal states) level. Federal lawmakers used their exclusive competence to regulate foreign affairs[147] and established the Federal Intelligence Service (*Bundesnachrichtendienst:* BND)[148] as the foreign intelligence ser-

---

[145] On this, see *Gusy*, ZRP 1987, 48; *Nehm,* NJW 2004, 3292; *Singer*, Die Kriminalpolizei 2006, 87.

[146] BVerfG NJW 2013, 1503; see also BVerfG NVwZ 1998, 497; for a historical background of the separation principle, see *Singer*, Die Kriminalpolizei 2006, 86; *Gusy*, KritV. 1994, 242; arguing for a constitutional foundation of the separation principle, *Gusy*, ZRP 1987, 45 ff.; *Daun*, Die deutschen Nachrichtendienste, 69; *Korte*, Informationsgewinnung der Nachrichtendienste, 59; *Roggan*/*Bergmann*, NJW 2007, 876; opposing a constitutional foundation of the separation principle, *Nehm*, NJW 2004, 3292.

[147] Art. 73 para 1 no 1 Basic Law; see also BVerfG NJW 2000, 59.

[148] Art. 87 para 1 Basic Law; § 1 para 1 BND-Gesetz.

vice of the federal government for the collection of foreign intelligence.[149] The Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz:* BfV) was established under federal law based on the exclusive competence of the federation for the protection of the constitution but is required to cooperate with the *Länder*.[150] Despite its somewhat unusual name for an intelligence service, the BfV is simply the federal domestic intelligence service, which is subordinate to the Federal Ministry of the Interior.[151] Federal law also provides for the Military Counterintelligence Service (*Militärischer Abschirmdienst:* MAD), responsible for efforts and activities involving the armed forces.[152]

Aside from the exclusive legislative competence of the federation, the *Länder* have the power to legislate based on their own constitutions.[153] In the area of internal security, the *Länder* established by statute 16 State Offices or Departments for the Protection of the Constitution (*Länderverfassungsschutzämter- oder Abteilungen*); thus, a total of 17 federal and state (*Länder*) agencies are engaged in domestic intelligence activities in Germany.[154] This paper will focus on the federal domestic intelligence service (BfV). In fact, by defining the framework of cooperation between the federal domestic intelligence service and the *Länder* services the federal lawmakers also established the range of required domestic intelligence activities.[155] The domestic intelligence services of the *Länder* must meet the requirements of this federal cooperation framework under federal law. However, the areas of responsibility and the powers of the *Länder* services may exceed this minimum requirement.[156] Moreover, the individual laws of the domestic intelligence services at the *Länder* level vary in different ways, for instance in their definitions of the agencies' areas of responsibility (*Aufgabenbereich*). For purposes of this paper, these differences will be discussed whenever they are important and pertinent. One example involves the limits of information sharing between the intelligence services of the Federal government and of the *Länder,* and the criminal prosecution

---

149 § 1 BND-Gesetz; see also *Gusy*, § 1 BND-Gesetz, at 1.

150 Art. 73 para 1 no 10 b and c, Art. 87 para 1 Basic Law; see also *Graulich*, Sicherheitsrecht des Bundes, 1.

151 § 2 para 1 of BfV-Gesetz.

152 Art. 73 para 1 no 1; I exclude the MAD in this context as it is of no importance for purposes of this publication, which focuses mainly on intelligence in general and crime control regarding civilians; on the MAD, see *Daun*, Die deutschen Nachrichtendienste, 59 and 63 ff.

153 Art. 70 para 1 Basic Law; § 2 para 1 BfV-Gesetz.

154 On the general structure of services, see also *Rose-Stahl*, Recht der Nachrichtendienste, 15.

155 *Graulich*, Sicherheitsrecht des Bundes, 2.

156 *Graulich*, Sicherheitsrecht des Bundes, 9; see also below III.A.1.c) Federal Office for the Protection of the Constitution (BfV).

authorities.[157] Finally, the federal intelligence service has the power to take the leading position—in consultation with the *Länder* service in charge—in cases of supra-regional scope and federal importance.[158]

In the following we will outline the areas of responsibility and the key characteristics of investigations conducted by the BND and the BfV (bb). Subsequently we will show how these investigations differ from preventive and repressive policing activities as defined by the conventional concepts of the security-related branches (cc).

### *b) Federal Intelligence Service (BND)*

The BND collects information on incidents that occur abroad and are relevant to German foreign policy and security policy.[159] The main focus of the security policy in terms of foreign countries is Germany's sovereignty and self-determination.[160] The security policy, which sets the objectives for intelligence gathering, is based on values and on the definition of the national interest, which in turn depends on the analysis of the current security environment.[161]

Observation targets of the BND are distinct in that they principally include all types of actions, circumstances, and persons. Normative considerations such as unlawfulness, the assignability of danger to a person as the causal agent or in some other capacity are not binding criteria for its investigations.[162] Such considerations would always run counter to the BND's mandate, which is precisely to act on its own initiative in the pre-field of any specific act and to initiate investigations in order to secure points of departure or links to existing security policy-related matters.[163] This very trait enables the BND to collect, at the earliest possible stage, information on events that might later turn into a suspicion of a concrete danger or a crime. Thus, intelligence gathering activities by the BND are based on the principle of relevance (*Sachbezogenheit*): the only requirement for an observation target is be security policy-relevant. More specifically, the relevance of respective targets for an intelligence gathering activity depends on how suitable and necessary they are for the agency's task.[164] This justifies intelligence gathering on targets not only

---

157 For more see below IV.B.2.a) General Framework.

158 See for more § 5 of BfV-Gesetz.

159 §§ 1 para 2, 2 para 1 no 4 BND-Gesetz; see also Art. 73 No 1 Basic Law; for the information collection process by the BND see *Daun*, Die deutschen Nachrichtendienste, 60.

160 BVerfG NJW 2000, 60 and 63; for more see *Gusy*, § 1 BND-Gesetz, at 26 ff.; *Paeffgen*, StV 1999, 669.

161 Weißbuch (2016), 15; *Daun*, Die deutschen Nachrichtendienste, 58 ff.; *Gusy*, § 1 BND-Gesetz, at 40; BVerfG NJW 1971, 280; BVerfG NJW 2000, 62.

162 *Gusy*, § 1 BND-Gesetz, at 32.

163 *Gusy*, § 1 BND-Gesetz, at 35; see also *Paeffgen*, StV 1999, 670.

164 See also § 2 para 1 BND-Gesetz; see also BVerfG NJW 2000, 63.

for purposes of countering identified threats but also for supporting the counteraction or even for establishing any relevance at all. Thus, the BND is authorized to gather information merely for purposes of 'extracting suspicion' (*Verdachtsgewinnung*) or establishing relevance, respectively, in advance of any specifically identified importance (so-called 'vacuum-cleaner-model').[165] The factual requirement, however, is conditioned on a temporal requirement insofar as the necessity for observation must be identifiable in terms of relevance.[166] Thus, the random observation of everything and everyone is not permitted. This is an important limitation on the intelligence services' information gathering expressly called for by the Federal Constitutional Court.[167] In contrast, the elements of relevance and suitability, constituting the only material investigation threshold for the BND, can be inferred from the experience of the service which also includes subjective assumptions.[168] In this regard, investigations by the BND require the least 'factual' basis for the probability judgment (*Wahrscheinlichkeitsurteil*)[169] as regards the relevance and necessity of specific information targets in order to carry out the BND's tasks.[170] Aside from this limited material condition, the BND's threshold for intervention (*Einschreitschwelle*) does not require other factual specifications (*anlasslos*) either in terms of time or person.

### *c) Federal Office for the Protection of the Constitution (BfV)*

Compared to the responsibilities of the BND, the objectives of the domestic intelligence service BfV, namely the protection of the state and the constitution, are more defined. They are the protection against

- unconstitutional efforts at home,
- activities of foreign intelligence services,
- violence-prone efforts that might jeopardize the external interests of the state, and
- efforts in conflict with the idea of international understanding or the peaceful coexistence of people.[171]

---

[165] *Paeffgen*, StV 1999, 669; *Gusy*, § 1 BND-Gesetz, at 59; see also BVerfG NJW 2006, 1944 ff.

[166] *Gusy*, § 2 BND-Gesetz, at 7; see also BVerfG NJW 2000, 63.

[167] BVerfG NJW 2000, 63; *Gusy*, § 1 BND-Gesetz, at 34; for the constitutional requirements of proportionality see also above II.B.2. The Proportionality Test in Security Law.

[168] *Gusy*, § 2 BND-Gesetz, at 34.

[169] For more, see above II.B.2. The Proportionality Test in Security Law.

[170] BVerfG NJW 2000, 63; see also BVerfG NJW 2008, 832.

[171] Art. 73 para 1 no 10 b and c Basic Law; see also §§ 1 para 1, 3 para 1 BfV-Gesetz; BVerfG NJW 2016, 1783; BVerfG NJW 2008, 828; BVerfG NJW 2006, 1942; *Korte*,

The BfV's approach is based on the assumption that certain political efforts (*Bestrebungen*) or activities that threaten the free democratic basic order cause potential dangers, which must be detected at the earliest possible time but definitely before they cause real harm to the legal interests listed above.[172] This includes threats that are emerging, currently exist, or have not yet materialized and have not yet been investigated by the police, as the players behind the threats are acting in secret, are still preparing, or do not violate the public order. Thus, the BfV is typically regarded as an early *warning* system.[173]

For the BfV, the law not only provides a general description of its responsibilities but outlines the targets for observation and information gathering. These targets are: politically defined, target- and purpose-oriented efforts of groups of persons, directed against the aforementioned legal interests by means of defined behaviour patterns or by impairing or endangering these interests.[174] Here, too, the actions underlying the aforementioned efforts need not be illegal or punishable.[175] The same applies to persons affected by the various measures of intelligence investigations, who do not need to be suspected to engage in the aforementioned efforts in a legally irresponsible way.[176] The focus is on the potential threat emanating from these efforts for the legal interests subject to observation by the intelligence service.[177] The efforts under observation need not be some kind of systematic, strategic aggression against the constitutional order.[178] It is sufficient if these efforts are objectively directed against certain essential principles of the constitutional order in order to eliminate or override them.[179] Such efforts are considered extremist if they are undertaken with the aim to eliminate these principles in part or in whole, as these acts are outside the framework of a free democratic constitutional order.[180] In BfV practice, the types of extremism under observation are classified as

---

Informationsgewinnung der Nachrichtendienste, 42; *Graulich*, Sicherheitsrecht des Bundes, 5.

[172] BVerfG NJW 2013, 1504; BVerfG NJW 2008, 828; BVerfG NJW 1971, 278 ff.; *Graulich*, Sicherheitsrecht des Bundes, 3; *Rose-Stahl*, Recht der Nachrichtendienste, 21;

[173] BVerfG NJW 1971, 278; BVerfG NJW 2000, 60; BVerfG NJW 2013, 1504; *Rose-Stahl*, Recht der Nachrichtendienste, 21.

[174] § 4 para 1 a BfV-Gesetz; see also BVerfG NJW 1971, 276.

[175] BVerfG NJW 2008, 832.

[176] BVerfG NJW 2008, 837 (with regard to the intelligence services receiving account information from the banks).

[177] *Rose-Stahl*, Recht der Nachrichtendienste, 47.

[178] *Rose-Stahl*, Recht der Nachrichtendienste, 52.

[179] These principles are: sovereignty of the people, principle of separation of powers, lawmaker bound by the constitutional order, legality of administration and judiciary, right to create and exercise a parliamentary opposition, changeability and responsibility of government, independence of the courts, exclusion of all types of tyranny and arbitrary rule, inclusion of human rights as specified in the constitution [§ 4 para 2 BfV-Gesetz].

[180] BVerfG NJW 1971, 278; *Rose-Stahl*, supra note 177, 50.

leftist, rightist, foreign, and sectarian groups.[181] On the one hand, extremism is more than political efforts that are violent or use terrorism as a tool for reaching their political goals,[182] which is why extremism as such covers actions that are in the pre-field of any specific danger or a crime.[183] On the other hand, extremism is not radicalism. The latter may include political efforts that are not compatible with the current constitutional order but can be tolerated as democratically stated opinions.[184] The demarcation between radicalism and extremism is an important borderline for observations by the BfV, even though this determination is not always evident at first sight. Finally, to start an investigation against a group or a person,[185] the BfV must confirm the presence of factual indications (*tatsächliche Anhaltspunkte*) of anti-constitutional efforts and the necessity for clarification.[186] However, a concrete suspicion that the efforts are anti-constitutional is not required.[187]

### *d) Main Features of Intelligence Investigations and Differences from Preventive and Repressive Police Investigations*

The criteria outlined above raise the issue of when any involvement by the BND or the BfV is justified at all. The law prescribes qualified thresholds for conducting certain investigative measures.[188] In compliance with the above-outlined spectrum of pre-field responsibilities, the intelligence services have far-reaching information gathering powers without a specific definition regarding the content of information gathering but also without a detailed regulation regarding the means to be used in the individual case.[189] For instance, in certain cases the BND is authorized to conduct what is called strategic surveillance in order to search the international telecommunication traffic for specific search terms (*Suchbegriffe*). In most cases, these terms are selected by the BND itself.[190] The regulations covering the methods and instruments of secret information gathering for use by the domestic intelligence services are quite general and do not depend on the content of the investigation. Examples are observations, the use of undercover informants, image and sound

---

[181] *Albert*, Informationsverarbeitung durch Nachrichtendienste, 95.

[182] *Rose-Stahl*, Recht der Nachrichtendienste, 50.

[183] BVerfG NJW 2013, 1504; BVerfG NJW 2008, 828; *Gusy,* Polizei- und Ordnungsrecht, 21; *Graulich*, Sicherheitsrecht des Bundes, 5; *Rose-Stahl*, supra note 181, 22.

[184] *Rose-Stahl*, Recht der Nachrichtendienste, 52.

[185] § 4 of BfV-Gesetz.

[186] *Rose-Stahl*, Recht der Nachrichtendienste, 68.

[187] BVerfG NJW 2008, 832.

[188] *Gusy*, § 1 BND-Gesetz, at 42.

[189] BVerfG NJW 2013, 1504; see also *Graulich*, Sicherheitsrecht des Bundes, 5.

[190] For the requirement of a reasoned notion and oversight by the parliamentary control committee, see § 5 para 1 BND-Gesetz; see also BVerfG NJW 2000, 63.

recordings, and manipulated papers or vehicle plate numbers.[191] These powers reflect the broad scope of responsibilities of the intelligence services and are characterized by relatively low intervention thresholds (*Eingriffsschwellen*).[192] As already mentioned above, the fact that intelligence services start their investigations at the earliest possible time is justified by the argument that the legal interests that might be targeted and harmed are those most important to the legal order.[193] The law does not stipulate significant restrictions on the intelligence agencies as to when they may start the observation, as long as the activities or efforts under observation are of substantial relevance and there is no misuse of power and gross breaches of the proportionality principle.[194] This principle prohibits, for instance, information gathering on what is called the core area of private life (*Kernbereich privater Lebensgestaltung*) by surveillance measures, as such an inference would touch on the essence of human dignity, which cannot be justified by any objective.[195] Aside from rather rare limitations such as this, the agencies enjoy a wide margin of discretion and are allowed to act according to their considerations of expediency when it comes to define their targets and start and complete their investigations.

Moreover, information gathering by the intelligence services is principally conducted in secret.[196] The services are not subject to the principle of openness in information gathering and are largely exempt from the requirements of transparency and notification of affected individuals.[197] Accordingly, the possibilities for individual legal protection against information gathering by the services are few and far between. In some cases, political control has completely replaced the legal protection by the courts.[198] Furthermore, the law equips the intelligence services with long-term and comprehensive surveillance measures that may target individuals indiscriminately.[199] An obvious example are mass surveillance

---

191 See for instance § 8 II BfV-Gesetz; BVerfG NJW 2013, 1504.

192 BVerfG NJW 2013, 1504.

193 BVerfG NJW 2000, 63; BVerfG NJW 2010, 841; see also BVerfG NJW 2006, 1942; BVerfG NJW 2008, 829; BVerfG NJW 2016, 1784; *Rose-Stahl*, Recht der Nachrichtendienste, 69.

194 § 2 para 4 BND-Gesetz; § 8 para 5 BfV-Gesetz.

195 For the constitutional meaning and scope, see BVerfG NJW 2016, 1786 ff. (surveillance measures by the Federal Criminal Police Office); BVerfG NJW 2004, 1002 (so-called residential surveillance for purposes of criminal investigations).

196 BVerfG NJW 2013, 1504; BVerfG NJW 1971, 276.

197 BVerfG NJW 2013, 1504; *Korte*, Informationsgewinnung der Nachrichtendienste, 41; see also *Singer*, Die Kriminalpolizei 2006, 86.

198 BVerfG NJW 2016, 1788; BVerfG NJW 2013, 1504; for the control of the parliamentary control committee and the so-called G 10-commission over telecommunication surveillance by the intelligence services, see Art. 10 para 2 Basic Law and §§ 14 and 15 G 10–Gesetz; for the constitutionality of this restriction, see BVerfG NJW 2016, 1788.

199 *Korte*, Informationsgewinnung der Nachrichtendienste, 53; *Albert*, Informationsverarbeitung durch Nachrichtendienste, 98.

measures.[200] In addition to long-term observations, the services also use different types of record-keeping and evaluation procedures. Not only are their databases more comprehensive, but their analysis is also different from conventional police investigations. A typical operating technique of the services is to look for some pattern in the targeted person's conduct and to search their own databases for matches. The services use these computer-based comparative systems particularly for counter-espionage purposes.[201]

In return and to compensate for the broad scope of information gathering powers of the intelligence services, their objectives for investigations are limited, essentially to the monitoring and reporting of fundamental threats that may destabilize society as a whole. Their reports are provided to the political decision makers in charge of security policy.[202] It is generally accepted that German law does not provide for a domestic 'secret service' (*Geheimdienst*) entitled to use coercive powers in the course of its duty.[203] A secret service would, for instance, be actively involved in combating terrorism. In fact, German law literally calls these agencies 'intelligence services' (*Nachrichtendienste*) or 'Office for the Protection of the Constitution' (*Amt für Verfassungsschutz*) rather than secret service agencies.[204] Therefore, the investigative objective of the intelligence services is not to actively fight against threats but to support the state bodies in their political assessments.[205] Against this background, it is not the responsibility of the BND to combat criminal offences as such but to generate intelligence including intelligence on criminal acts committed abroad and important in terms of the foreign and security policies of the Federal Republic of Germany.[206] The same is true for the domestic intelligence services. Their investigations are also not *directly* aimed at the prevention of and defence against specific crimes and the preparation of respective operative measures in the context of anti-constitutional extremism.[207] However, this does not mean that the intelligence services avoid persons as targets involved in activities constituting a security threat. On the contrary, they are interested in collecting information on all persons involved, whether associated, affiliated, or connected, and on all kinds of involvement regardless of whether the actions of the individuals involved are legal

---

200 On this, see *Korte*, Informationsgewinnung der Nachrichtendienste, 38.

201 *Albert*, Informationsverarbeitung durch Nachrichtendienste, 103.

202 BVerfG NJW 2013, 1504; BVerfG NJW 2000, 60.

203 *Gusy*, § 1 BND-Gesetz, at 23.

204 On this, see also *Rose-Stahl*, Recht der Nachrichtendienste, 18; *Albert*, Informationsverarbeitung durch Nachrichtendienste, 68, 88, and 98; *Korte*, Informationsgewinnung der Nachrichtendienste, 51 ff.

205 BVerfG NJW 2000, 60; BVerfG NJW 2013, 1502; *Gusy*, § 1 BND-Gesetz, at 29.

206 BVerfG NJW 2013, 1504; BVerfG NJW 2000, 63.

207 BVerfG NJW 2013, 1504.

or illegal.[208] The most distinctive feature is the fact that the intelligence services are not bound to investigate conduct described by law as illegal or a crime. As said above, the balancing factor is that the intelligence findings will provide the foundation for measures that will be taken to address the perceived dangers at the political level.[209] Based on the nature of this function, the intelligence services are not considered law enforcement agencies. Both the BND-Law and the BfV-Law explicitly state that the intelligence agencies may not be attached to a police authority.[210] Compared to preventive and repressive police investigations, intelligence investigations do not impose external coercive measures.[211] Likewise, both the BND-Law and the BfV-Law explicitly stipulate these constitutionally and conceptionally prescribed features, specifically that the agencies do not have policing powers (*polizeiliche Befugnisse*).[212] Against this background, any such measure against an individual is neither intended nor allowed.[213] The Federal German Constitutional Court emphasizes that the lack of operational power distinguishes these intelligence services from the secret police (*Geheimpolizei*).[214] In most cases, targeted persons have the opportunity to withdraw from intelligence gathering, which means that, in such cases, the intelligence services have no way of imposing an information gathering process on the person, such as search or seizure,[215] arrest, or interrogation.[216] Finally, the intelligence services are neither compelled to investigate not are they allowed to file a charge.[217]

The limited responsibilities and objectives of the intelligence services outlined above can also be seen in the limits on their cooperation with other authorities: the intelligence services are not entitled to resort to policing powers nor can they ask the police for respective measures by way of administrative cooperation (*Amtshilfe*).[218] Similarly, any response to requests by other public authorities may, *in principle*, only result in the transfer of information the intelligence services already know or that can be gathered from publicly available sources.[219] However, even

---

[208] See *Korte*, Informationsgewinnung der Nachrichtendienste, 50 and 53.

[209] BVerfG NJW 2013, 1502.

[210] § 1 para 1 BND-Gesetz; § 2 para 1 BfV-Gesetz.

[211] *Korte*, Informationsgewinnung der Nachrichtendienste, 45; *Nehm,* NJW 2004, 3289.

[212] § 2 para 3 BND-Gesetz, § 8 para 3 BfV-Gesetz; see also *Gusy,* Polizei- und Ordnungsrecht, 21; *Graulich*, Sicherheitsrecht des Bundes, 7; *Singer*, Die Kriminalpolizei 2006, 86; *Roxin*/*Schünemann*, Strafverfahrensrecht, 63.

[213] *Gusy*, ZRP 1987, 48.

[214] BVerfG NJW 2013, 1505.

[215] *Korte*, Informationsgewinnung der Nachrichtendienste, 49 ff.

[216] *Albert*, Informationsverarbeitung durch Nachrichtendienste, 92.

[217] *Korte*, Informationsgewinnung der Nachrichtendienste, 53 ff.

[218] § 2 para 3 BND-Gesetz, § 8 para 3 BfV-Gesetz; BVerfG NJW 2013, 1504.

[219] § 17 para 1 BfV-Gesetz; § 24 para 3 BND-Gesetz; BVerfG NJW 2013, 1504.

within the boundaries of the conventional concept, the Federal Constitutional Court accepts that information gathering by the BND or the BfV 'at least indirectly' serves to prevent, investigate, or prosecute certain crimes, even though the principal suppliers of the information, namely the intelligence services and their strategic monitoring, do not share this primary objective.[220] In fact, the conventional concept of the security branches does not prohibit all types of cooperation between the intelligence services and the police.[221] Intelligence information not infrequently serves to impose preventive police measures in a broad sense, particularly in immigration law or the right-of-assembly law.[222] The sharing of information between the federal intelligence services and the criminal prosecution authorities will be discussed in more detail below.[223]

## 2. Police

### *a) Structure*

According to the conventional concept of policing, the duties of the police are either preventive (*Gefahrenabwehr*) or repressive (*Strafverfolgung*). The regulation of the responsibilities and the organization of the police are also subject to the federal organization of the state: the legislative competence is with the federation, provided the Basic Law does not confer this power on the federal states (*Länder*).[224] Based on this constitutional division of competences, the federal lawmaker enacts preventive police law to the extent the constitution explicitly states a duty to prevent, or the duty to prevent must be regulated as an annex to a subject matter over which the federation has legislative competence: customs, the exchange of goods and payments with foreign countries including customs and border protection, air transport, railways, or telecommunications are examples of matters where the respective federal legislations also include preventive regulations aimed at preventing or taking precautions against dangers or related legal interests in these areas.[225] Other than this preventive law, which the federal legislature introduced as subsidiary legislation, it is typically the *Länder* that exercise legislative powers

---

[220] BVerfG NJW 1971, 280.

[221] *Gusy*, ZRP 1987, 49; *Korte*, Informationsgewinnung der Nachrichtendienste, 59.

[222] See for instance BVerwG NVwZ 2005, 1435; VG Braunschweig Decision dated 27 Oct. 2011 – 5 B 164/11 BeckRS 2011, 55396.

[223] See for more IV.B. Transfer and Use of Intelligence Information at the Investigation Stage.

[224] Art. 70 para 1 Basic Law; see also *Gusy,* Polizei- und Ordnungsrecht, at 38.

[225] Art. 73 paras 5 and 7 Basic Law; see also BVerfG NJW 2004, 2214; BVerfG NJW 2010, 837.

over preventive police tasks.[226] The same principle applies to repressive police investigations: the federation exercises the so-called concurrent legislative power over criminal law, the organization of the court, and criminal procedure, including police investigations based on suspicion of a committed criminal offence;[227] *inter alia* the Penal Code (StGB; in English: PC) and the Code of Criminal Procedure (StPO; in English: CCP) are products of an exhaustive exercise of this federal competence. Consequently, the *Länder* do not have legislative competence in the areas of substantive and procedural criminal law, where their regulations are superseded by federal law.

Regarding the execution of federal preventive and repressive police law, the federal legislative power is subordinate to that of the *Länder* when it comes to establishing police agencies: the execution of federal law is assigned to the *Länder* authorities to the extent the Basic Law does not provide otherwise.[228] In order to implement preventive and repressive police law related to the above-mentioned areas, the federal lawmakers established *inter alia* the federal police (*Bundespolizei*: BP) and the customs criminal investigation office (*Zollkriminalamt*: ZKA), including local customs investigation offices (*Zollfahndungsämter*: ZFA).[229] In 2006, the federal legislature was granted the new exclusive legislative power to provide for the prevention of dangers of international terrorism.[230] The Federal Criminal Police Office (*Bundeskriminalamt:* BKA), which was originally in charge of repressive police investigations in matters of national importance, has since also been tasked with the prevention of international terrorism.[231] Aside from the police agencies subsidiarily established by the federal lawmakers, the *Länder* exercise ordinary legislative power to establish *Länder* police authorities for the execution of preventive and repressive laws at the federal level and at the *Länder* level.[232] These authorities are organized as the *Länder* police forces (Landespolizei: LP) and the *Länder* criminal police offices (Landeskriminalämter: LKA).

Finally, the *Länder* are the principal regulator of preventive police law: there are 16 *Länder* police codes in Germany. Federal law has an additional three (major) preventive police codes in the areas of international terrorism, customs, and border

---

[226] Art. 30, 70 para 1, 83 Basic Law; *Gusy,* Polizei- und Ordnungsrecht, 38; *Roxin*/*Schünemann*, Strafverfahrensrecht, 63.

[227] Art. 74 para 1 no 1 Basic Law.

[228] Art. 83 Basic Law; see also Art. 30 Basic Law; Gusy, Polizei- und Ordnungsrecht, 38.

[229] On the federal police authorities, see *Gusy,* Polizei- und Ordnungsrecht, 38 ff.; *Daun*, Die deutschen Nachrichtendienste, 70; *Roxin*/*Schünemann*, Strafverfahrensrecht, 63 ff.

[230] Art. 73 para 1 no 9a Basic Law.

[231] For more, see *Roggan*, NJW 2009, 257.

[232] Arts 30, 70 paras 1, 83 Basic Law; *Gusy,* Polizei- und Ordnungsrecht, 38; *Roxin*/*Schünemann*, Strafverfahrensrecht, 63.

protection. Whereas the federation regulates predominantly repressive criminal law and procedural law, the *Länder* police authorities mostly enforce criminal law.

### *b) Preventive Policing*

Pursuant to the preventive police codes of the *Länder*, the principal general responsibilities of the police authorities are to protect public security, the public order, private rights, and to provide law enforcement assistance to other public bodies.[233] Of these, public security is the most widely used justification and obligation for preventive policing.[234] Its definition is the first step in defining the responsibilities of the preventive police forces. Public security is generally considered to consist in the protection of all the interests the legal system recognizes through statutory laws,[235] which can then be divided into public and individual interests. The core areas of public legal interest are the existence of the state and its ability to function, including the integrity of its institutions.[236] The second group of interests incorporates primarily the individual interests in life, limb, health, honor, and property.[237]

The scope of protection for public and individual interests is defined in the negative by the respective offences under criminal law, as such an offence would clearly violate these interests. However, preventive police law transcends the area of criminal activity in that its protective scope already includes, in a general sense, an *anticipated endangerment* of the public and individual legal interests in *future* with the aim of preventing danger (*Gefahrenabwehr*) or, if harm has already occurred, with the aim of removing the disturbance (*Störungsbeseitigung*). Moreover, the scope of preventive police law and, as such, the power of the police to interfere with the basic rights and freedoms of a suspected 'endangerer' (*Gefährder*) or 'disturber' (*Störer*) is defined by the objective nature of this area of the law. In the latter case this means not only that the so-called 'endangerer' or 'disturber' does not need to cause harm or danger to a protected legal interest in the presence of a certain 'mens rea'; it means that, given certain conditions, measures of preventive po-

---

233 See for instance §§ 1, 2 Baden-Wuerttemberg Police Law; § 1 Bavarian Police Law; § 1 North Rhine Westphalian Police Law.

234 For purposes of this publication, the notion of public order seems to be less important. It is generally understood as the sum of uncodified norms whose observance is regarded as an indispensable prerequisite for an orderly human coexistence; social norms must be counted as such (for more, see *Gusy,* Polizei- und Ordnungsrecht, 48 ff.). The importance of the protection of the public order has been growing recently, especially in the political framework of internal security: for instance, the government emphasizes its protection by the police (Weißbuch (2016), 39).

235 *Gusy,* Polizei- und Ordnungsrecht, 40.

236 BVerwG NVwZ 2017, 1534; BVerwG NJW 2012, 2677; *Gusy,* Polizei- und Ordnungsrecht, 41.

237 BVerwG NJW 2012, 2677; *Gusy,* Polizei- und Ordnungsrecht, 42.

lice law may also be directed against a third party who did not even contribute causally to the development of harm or danger.[238] Furthermore, the scope of preventive police law is influenced by the definition of danger.[239] In fact, this notion is at the heart of the temporal boundaries of preventive police law: the brief definition of danger within the meaning of preventive police law is 'foreseeable future harm'. According to the long definition, danger must be assumed where there is sufficient likelihood that circumstances or a specific behaviour will be such as to cause harm to a legal interest protected under police law if the circumstances or conduct progress as objectively expected and the police does not intervene.[240] This is the commonly accepted definition of concrete danger, which—in accordance with police law as it is conventionally understood—imposes limits on preventive police investigations. Furthermore, the scope of preventive police law is determined by the notion of harm. The law clearly does not cover all types of anticipated infringements on a protected legal interest. It is not always easy to separate unlawful harm from socially adequate, tolerable, or negligible infringements.[241] In the context of the harm requirement, it must be emphasized that there are a number of inherent uncertainties in preventive police law, because it attempts to address harm that is only expected in future.[242] Not least due to this fact, as long as police actions remain within the boundaries of preventing danger, it is at the discretion of the police whether to start investigations and how to conduct them (principle of facultative action).[243]

### *c) Repressive Policing*

The Federal Code of Criminal Procedure (CCP) also requires police authorities and police officers responsible for preventing danger (*Gefahrenabwehr*) to investigate on suspicion that a crime has been committed.[244] In this capacity, the police assist in the criminal prosecution under the supervision of the public prosecutor in charge. In certain scenarios explicitly regulated by statute, the public prosecutor is also responsible for taking precautionary measures for a criminal investigation in

---

238 See for instance BVerfG NJW 2016, 1786 (with regard to surveillance of the contact persons or message intermediators); compare, however, with the jurisprudence of the German Constitutional Court on the constitutionality of police investigation measures targeting an unspecified group of people BVerfG NJW 2008, 1507 f.; BVerfG NJW 2012, 1424 ff.

239 *Gusy,* Polizei- und Ordnungsrecht, 52.

240 *Gusy,* Polizei- und Ordnungsrecht, 53 ff.; *Chalkiadaki*, Gefährderkonzepte in der Kriminalpolitik, 21 ff.

241 For more, see *Gusy,* Polizei- und Ordnungsrecht, 53 ff.

242 *Gusy,* Polizei- und Ordnungsrecht, 57.

243 *Gusy,* Polizei- und Ordnungsrecht, 239.

244 § 163 para 1; *Gusy,* Polizei- und Ordnungsrecht, 76.

the future even though there is no criminal investigation based on an initial suspicion.[245]

In their criminal investigative duties, the police are subordinate to the public prosecutor and must follow and carry out his or her instructions.[246] In practice, however, it is typically the police who initiate an investigation, carry out measures, and present the results of the investigation to the public prosecutor in charge. Although the latter officially leads the investigation and determines the course of investigation, he or she intervenes only in the more important cases.[247] Police officers designated by the *Länder* governments as investigative staff in criminal prosecutions make up the criminal investigation departments of the local police; compared with ordinary police officers, these officers have more powers in criminal investigations, for example to conduct searches and seizures.[248]

The police are required to 'take action regarding all prosecutable criminal offences, provided there are sufficient factual indications'.[249] This requirement is the foundation for the justification and obligation to investigate (the so-called initial suspicion: *Anfangsverdacht*) and must be based on specific circumstances. This means that vague or mere assumptions cannot meet this threshold.[250] However, the suspicion itself, which the police will have inferred from the factual indications, does not need to be particularly strong or qualified.[251]

The police may obtain factual indications from the report of a victim, witness, other public institutions, or open public sources (the news or social media) or may come across respective circumstances in the course of their own actions unrelated to the specific suspicion.[252] However, the police are prohibited to start investigations on their own initiative in order to detect any factual indications in the first place. This is why so-called pre-field investigations (Vorfeldermittlungen) for purposes of criminal prosecution are not allowed.[253] Similarly, the threshold of initial suspicion must not be bypassed by police actions allegedly conducted in perfor-

---

[245] Meyer-Goßner/*Schmitt*, § 163 (StPO) at 17.

[246] § 152 I Court Constitution Act (Gerichtsverfassungsgesetz); Meyer-Goßner/*Schmitt*, § 153 (GVG) at 1; *Roxin*/*Schünemann*, Strafverfahrensrecht, 60.

[247] *Roxin*/*Schünemann*, Strafverfahrensrecht, 61; *Gusy,* Polizei- und Ordnungsrecht, 76.

[248] Meyer-Goßner/*Schmitt*, § 153 (GVG) at 1; *Gusy,* Polizei- und Ordnungsrecht, 76; *Roxin*/*Schünemann*, Strafverfahrensrecht, 60.

[249] § 152 para 1.

[250] Meyer-Goßner/*Schmitt*, § 152 (StPO) at 4; see also above II.B.2. The Proportionality Test in Security Law.

[251] Meyer-Goßner/*Schmitt*, § 152 (StPO) at 4.

[252] See § 160 para 1 StPO; *Gusy,* Polizei- und Ordnungsrecht, 76.

[253] Meyer-Goßner/*Schmitt*, § 152 (StPO) at 4b; on pre-field investigations in preventive police law, see BVerfG NJW 2005, 2610; see also below III. B. 1. General Overview: Restructuring the Security Architecture.

mance of non-criminal duties but actually intended to investigate indications of assumed crimes. Moreover, as soon as the existence of an initial suspicion is no longer in doubt, the police must follow criminal procedure law and inform the suspect about his or her rights.[254] Except for these limitations, there are certain steps the police may take themselves to clarify the probative value of the indication available, such as questioning people on what they know, before investigations are officially initiated, including the opening of a criminal file in a specific case.[255]

The principle of mandatory prosecution is, *inter alia*, a guide for criminal prosecution.[256] Thus, not only are the police and the public prosecutor compelled to investigate in the presence of 'sufficient factual indications', but the prosecutor must also file a public charge if the outcome of preliminary investigations provides 'sufficient reason' for it.[257] The rationale behind the principle of mandatory prosecution is that the democratically elected parliament, not the administration, should decide whom to prosecute and punish. While this indicates a certain distrust of the administration, the rationale is also rooted in the principles of rule of law, certainty, and equality.[258] However, the principle of mandatory prosecution is not strictly applied. It is generally accepted that there may be circumstances where the principle of proportionality requires dropping the prosecution of a criminal case, conditionally or unconditionally.[259] Nevertheless, there is no general concept that serves as a foundation for all exceptions.[260]

#### *d) Overlaps between Preventive and Repressive Police Investigations*

Another conceptual problem is the relationship between preventive and repressive police investigations. Although both areas of the law aim at the protection of corresponding legal interests, the investigations are nevertheless subject to different temporal and material conditions. However, it is obvious that the prevention of harm and the prosecution of endangerment or harm that already occurred are quite close. This is even reflected in the fact that the same authority, the police, is responsible for both duties.[261] According to the conventional conceptualization of the

---

254 Meyer-Goßner/*Schmitt*, § 152 (StPO) at 3.

255 Meyer-Goßner/*Schmitt*, § 152 (StPO) at 4b, § 163 (StPO) at 9.

256 §§ 152 para 2, 163 para 1 StPO; see also *Vogel*, The Core Legal Concepts and Principles, 55 f.

257 Ibid.; see also *Roxin*/*Schünemann*, Strafverfahrensrecht, 79.

258 *Roxin*/*Schünemann*, Strafverfahrensrecht, 79; see *Brodowski*, Alternative Enforcement Mechanisms, 370 ff.

259 For exceptions, see *Vogel*, The Core Legal Concepts and Principles, 55 f.; *Brodowski*, Alternative Enforcement Mechanisms, 373 ff.; *Roxin*/*Schünemann*, Strafverfahrensrecht, 80 ff.

260 *Roxin*/*Schünemann*, Strafverfahrensrecht, 80.

261 *Roxin*/*Schünemann*, Strafverfahrensrecht, 59.

security branches, the separation of preventive police investigations and criminal prosecution does not cause substantial problems: the objective of preventive police law is not to prepare criminal proceedings and deal with past wrongdoings. Rather, it is about preventing or removing future harm.[262] As both objectives differ, an overlap problem does not seem to be possible. However, a closer look reveals quite the opposite.[263] The overlap between preventive and repressive police investigations becomes obvious when the preventive police first initiate investigations against so-called endangerers or disturbers who later enter the criminal arena by still causing harm. Take a group of hooligans or a person walking in a public space, knife in hand, and their later involvement in a fight with fans of a rivalling club or in the attack of a pedestrian. Second, even if the planning or preparation of certain crimes was not covered by preventive police investigations and the repressive police step in first for the purpose of criminal investigations based on an initial suspicion, subsequent police investigations with regard to a specific crime will not only aim at collecting evidence for the purpose of criminal prosecution and subsequent criminal trial but will also include preventive actions. This is particularly the case where the police investigate offences committed by a criminal network, group, or organization which is the focus of police prevention itself or through other persons connected with it. In fact, it is generally acknowledged that under such circumstances the criminal investigation should also be able to infiltrate the core of the criminal organization, uncover its structure, and even collect evidence against the most responsible lead actors, organizers, financiers, and masterminds. The point is that, in such cases, police investigations, whether preventive or repressive, are in fact interconnected such that all preventive and repressive efforts are aimed at breaking the circle of criminals.[264]

The above-mentioned cases raise the issue of what law applies to them and who will lead the investigations as the police may not use the powers of preventive police law to investigate based on a criminal suspicion nor the measures under criminal procedure law to thwart a danger.[265] The public prosecutor is the ‘master’ of the investigation stage as soon as a criminal prosecution is initiated. The police are not subordinate to the public prosecutor in carrying out their preventive duty; a chief police officer decides on the course of investigations.[266]

---

[262] *Gusy,* Polizei- und Ordnungsrecht, 53; *Chalkiadaki*, Gefährderkonzepte in der Kriminalpolitik, 17 ff.

[263] Generally, see *Chalkiadaki*, Gefährderkonzepte in der Kriminalpolitik, 24 ff.

[264] For more, see BVerfG NJW 2004, 2217; BVerfG NJW 2004, 1002 ff.; see also Meyer-Goßner/*Schmitt*, § 152 at 6; *Gusy,* Polizei- und Ordnungsrecht, 4.

[265] *Gusy,* Polizei- und Ordnungsrecht, 77.

[266] BVerfG NJW 2005, 2607.

### *e) Main Features of Police Investigations and Differences from Intelligence Investigations*

The police and criminal prosecution authorities are significantly different from the intelligence services in terms of their objectives, responsibilities, *modi operandi*, and methods. They are responsible for preventing, averting, and prosecuting crimes as well as preventing other dangers to public security and order.[267] Their responsibilities are characterized by operative actions and, in particular, by the power to carry out coercive measures against individuals.[268] As a result of a police investigation, affected persons may not only be subject to measures leading to considerable infringements on basic rights and freedoms, but the outcome of subsequent proceedings may also result in administrative or criminal sanctions. This is why the law is more restrictive when it comes to regulating police actions with regard to the prevention of danger or the prosecution of crimes. The legal regulations on the scope of their investigations are not only more specific but also provide an arsenal of investigative measures that vary both in terms of material and procedural requirements. Apart from some of the responsibilities these authorities have in the pre-field of danger as a matter of principle, measures against individuals are only authorized if there is a specific cause (*konkreter Anlass*). This typically requires the presence of indications to suspect a criminal act or a danger related to a specific event.[269]

The same thresholds that must be met for any involvement of the police also apply to information gathering. Because the collection of information may ultimately prepare and provide reasons justifying compulsive measures and therefore restrictions on basic rights and freedoms, the laws regulating police powers for information gathering are substantially tighter, more precise, more diverse than the powers of the intelligence services for information gathering.[270] Moreover, the police generally act in the open, and the collection of information also follows the principle of openness even though police investigations do include rather secret measures against individuals.[271] However, only certain investigative measures or stages are kept secret. The use of undercover agents or informants and secret information gathering techniques are only permitted as an exception and under certain conditions. The generally open nature of police work remains untouched. Further, the information gathered is disclosed to the affected person or suspect in subsequent procedures such as when the indictment is filed or a police order is

---

267 BVerfG NJW 2013, 1504; BVerfG NJW 2016, 1782.

268 *Singer*, Die Kriminalpolizei 2006, 86.

269 BVerfG NJW 2013, 1504.

270 BVerfG NJW 2013, 1504.

271 *Korte*, Informationsgewinnung der Nachrichtendienste, 47.

issued. This allows the affected person to take a stand against it. The open nature of investigations can be seen in the way in which other standard measures of criminal proceedings are conducted, such as searches and seizures, interrogations, or the inspection of case files as well as the invocation of other defence rights. More importantly, the trial court is principally conducted in public and orally.[272]

In sum, the German legal system generally distinguishes between a police force that, for the most part, acts openly, primarily carries out operational tasks, and is guided by a detailed legal framework, and intelligence services that essentially operate under cover, are limited to observations in the pre-field for the purpose of advising political decision-makers and are therefore operating on the basis of a less differentiated legal framework.[273] However, these distinctions are merely a preliminary approximation to the range of relationships between intelligence, preventive police, and criminal prosecution and do not provide the entire picture. Even within the conventional concept of the security branches, there are many different ways in which the investigations of the individual branches overlap.

### 3. Overlaps between Intelligence, Police, and Criminal Prosecution

According to the general concept outlined above, the intelligence services are responsible for investigations as early as in the pre-field of a specific danger or suspicion of crime.[274] Similarly, prevention precedes criminal prosecution. Thus, it appears that security is provided following the sequence of intelligence, prevention, and repression. However, a closer look reveals that the individual stages are not very clearly separated. Although intelligence investigations usually involve matters and actions irrelevant to preventive and repressive police, there are cases where relevance can be established not only *ex-post*, after the observed events or efforts have met the thresholds of specific danger or criminal suspicion, but also *ex-ante*, at the very beginning of intelligence observations. In both cases, parallel preventive or repressive investigations will not preclude or stop intelligence observations. One of the conventional overlap areas between intelligence and criminal prosecution involves offences against national security,[275] for instance, in case of espionage. In fact, the *modus operandi* of intelligence services in this context even resembles, to some extent, a criminal investigation as they are engaged in identifying individuals

---

[272] BVerfG NJW 2013, 1504; for more, see *Vogel*, The Core Legal Concepts and Principles, 57.

[273] BVerfG NJW 2013, 1502, and 1505.

[274] *Gusy*, ZRP 1987, 48; see also above III.A.1.d). Main Features of Intelligence Investigations and Differences from Preventive and Repressive Police Investigations.

[275] See § 3 para 1(a) BND-Gesetz.

involved in activities by hostile services. As a result, they gather information not only to start counter-operations but also to identify so-called backers, case officers, and traitors at home.[276]

As the gathering of information for purposes of national security and for the protection of the constitutional order in order to keep the government informed is considered to be the primary objective of intelligence investigations, the parallel jurisdiction of the intelligence service and the police in the cases mentioned is principally not challenged.[277] In fact, whenever the political assessment of the security situation in Germany is provided at the Office of the Chancellor, the presidents of the three federal intelligence services give their accounts on the security situation but so does the president of the Federal Criminal Police Office (BKA), and, occasionally, the Federal Prosecutor General (*Generalbundesanwalt*).[278] Also, it is not considered unusual for the intelligence services to request information from the police authorities before they specify their observation targets. This facilitates not only the definition of certain specific activities, networks, or milieus as observation targets but of individuals as well.[279] In fact, the police traditionally have their own 'state protection' departments (*polizeilicher Staatsschutz*), which reveals a close overlap with the intelligence services in terms of the preventive and repressive fight against national security offences.[280] Finally, the way the security branches are conventionally conceived, the strategic intelligence they provide in their political briefings of decision-makers through strategic intelligence also includes analyses of the security situation in general for the police and criminal prosecution authorities so as to draw their attention to current security concerns.[281] However, the intelligence services have broad discretion as far as cooperation beyond this general framework is concerned, especially in terms of informing the police on specific cases or transmitting intelligence as evidence. Certainly, the services are not only interested in information gathering and passively monitoring criminal activities such as espionage but also in cracking down on espionage networks and in the criminal prosecution of the perpetrator. Still, as for sharing their knowledge with the criminal prosecution authorities, they are not bound by the principle of legality

---

276 *Albert*, Informationsverarbeitung durch Nachrichtendienste, 95.

277 *Gusy*, ZRP 1987, 48.

278 *Daun*, Die deutschen Nachrichtendienste, 62 ff.

279 *Albert*, Informationsverarbeitung durch Nachrichtendienste, 96.

280 For more on the state protection departments und the way they work, see *Abbe,* Der polizeiliche Staatsschutz und seine Datenbanken. [https://police-it.org/der-polizeiliche-staatsschutz-und-seine-datenbanken]; on information gathering by state protection departments, see for instance 'Göttinger Staatsschutz soll illegal Daten erhoben haben', *Spiegel Online* 16 June 2017, available at: http://www.spiegel.de/panorama/justiz/goettingen-polizei-soll-illegal-daten-erhoben-haben-a-1152428.html.

281 *Albert*, Informationsverarbeitung durch Nachrichtendienste, 105.

but enjoy broad discretion on questions of whether they will ever share their knowledge and when they do so.[282] This issue will be addressed in more detail below.[283]

## B. Reconfiguration in light of selected issues

### 1. General Overview: Restructuring the Security Architecture

In light of the constitutionally mandated principle of proportionality and the protection of basic rights and freedoms, the above-outlined conventional security concept has been challenged by measures of a new security law that have caused a substantial restructuring of the security architecture. There were departures from the conventional measures at many levels and in different ways, for instance the introduction of information gathering powers that exceed even the competence of the intelligence services. Prime examples are some areas in the data retention regulations,[284] such as data retention by telecommunication providers. Data retention is not only comprehensive and targets everyone indiscriminately but also occurs without any previously identifiable need or benefit for the intelligence services or any suspicion of a crime or specific danger.[285] In these cases information is gathered, to use the conventional terminology, in the pre-field of pre-fields.[286] This indicates that these data retention laws are predominantly defined by the contemporary precautionary security policy. Moreover, the intelligence framework was reconfigured: the areas of responsibility of the intelligence services were explicitly expanded to include the observation of certain crimes,[287] and the criminal prosecution authorities were increasingly granted access to intelligence information on crimes, including, *inter alia*, the recent establishment of a counter-terrorism database.[288] This process of converging occurred not only between intelligence services and criminal prosecution authorities. The intelligence services were granted these information gathering powers only because their objectives are the prevention of harm to life, limb, and freedom of individuals—which are legal interests typically protected by preventive police.[289]

---

[282] *Albert*, Informationsverarbeitung durch Nachrichtendienste, 95, note 13.

[283] For more, see IV.B. Transfer and Use of Intelligence Information at the Investigation Stage.

[284] For more, see *Tamm*, VuR 6/2010, 215–223.

[285] For more, see below III.B.2. Precautionary Data Retention.

[286] For more, see above III.A.1. b) Federal Intelligence Service (BND) and c) Federal Office for the Protection of the Constitution (BfV).

[287] See below III.B.3. At the Level of the Intelligence Services.

[288] BVerfG NJW 2013, 1499 ff.

[289] See above III.A.2.b) Preventive Policing.

A clear-cut example of the convergence of intelligence, preventive police investigations, and criminal prosecution is the Federal Financial Intelligence Unit. Although entities so obliged under statute are the first to collect, retain, and analyze information to assess the risks of certain transactions,[290] the Intelligence Unit is responsible for the prevention and prosecution of money laundering and terrorist financing in addition to conducting strategic analyses *inter alia* on grounds of transmitted suspicious transactions and for the compilation of reports.[291] In this context this Unit is not only authorized to suspend a transaction possibly related to money laundering or terrorist financing[292] but is obliged, on a case-by-case basis, to immediately transfer the outcomes of its analysis to the criminal prosecution authorities.[293]

In fact, the very concept of pre-field investigations (*Vorfeldermittlungen*) that traditionally characterized the *modus operandi* of the intelligence services has increasingly been incorporated into the fields of preventive police law and repressive criminal prosecution law.[294] Today, preventive and repressive police investigations are also permitted outside the boundaries of a specific danger or suspicion of a crime. This resemblance to intelligence investigations caused some scholars to claim that the police now clearly have an 'intelligence gathering' mandate.[295] In fact, the police have long been demanding more criminal intelligence not delivered to them by other administrative bodies but gathered on their own initiative and account.[296]

In particular, in addition to the category of 'specific danger' (*konkrete Gefahr*) or variations thereof such as 'current or pressing danger' (*gegenwärtige oder dringende Gefahr*), new thresholds have been defined that allow the police to take preventive measures in the pre-field of a specific event. The most far-reaching is the notion of abstract danger, where the boundaries between intelligence investigations and preventive police investigations all but disappear. The German Federal Constitutional Court rejected the application of such a threshold but accepted lower levels of danger, which certainly fall short of the standard of 'specific danger': 'threatening danger' (*drohende Gefahr*), 'continuing danger' (*Dauergefahr*), or 'common danger' (*gemeine Gefahr*) may serve as examples.[297] With regard to the definition of danger, the other striking development is that the Federal Court acknowledged that, in connection with terrorism, a determination predominantly focused on the circumstances of the individual case may be abandoned in favour of a concept of

---

290 §§ 2 ff. Money Laundering Law.

291 §§ 28 ff. Money Laundering Law.

292 § 40 para 1 Money Laundering Law.

293 § 32 para 2 Money Laundering Law.

294 See for instance BVerfG NJW 2005, 2610.

295 *Roggan*, NJW 2009, 262.

296 *Daun*, Die deutschen Nachrichtendienste, 68.

297 BVerfG NJW 2008, 831; BVerfG NJW 2016, 1784 ff.

danger more based on the nature of danger a person poses in terms of his or her views.[298] While this may be consistent with the Court in cases where a person travels from a terrorist training camp abroad to Germany, it will be difficult to sufficiently substantiate dangerousness in a person who has merely a strong affinity with a fundamentalist notion of religion.[299]

In fact, there is a noticeable trend towards the preventive powers of the police that justify acting against individuals based on their profile-based dangerousness. More specifically, so-called 'endangerers' of international terrorism and right-wing extremism are entered into databases[300] storing information from the intelligence, the police, and the criminal prosecution agencies.[301] It is noteworthy that these databases use administrative subcategories of 'endangerer' which are mirrored in certain terrorism offences of the Penal Code.[302]

The scope of preventive police law is also expanded by criminalizing particular preparatory acts that were previously not punishable.[303] On the one hand, the fact that these new offences exist authorizes the preventive police to start with the prevention of harm directed at legal interests also protected by these new preparatory offences. On the other hand, the criminal prosecution agencies may investigate as well, *inter alia* by using secret investigative techniques and measures of criminal procedure at a very early stage of preparing a crime, and may collect evidence.[304] Given that the wrongdoing of the perpetrators of these new offences consists mainly in a guilty mind, namely the intent to commit a more harmful act, the use of secret methods and investigative measures in order to expose a suspect's closed mindset is a conceptional necessity.[305] This entire development involves the risk of significantly expanding the—conventionally acknowledged—information gathering by the police for state protection purposes (*polizeilicher Staatsschutz*)[306] and of

---

[298] On the concept of "endangerer" with regard to terrorism generally, see *Chalkiadaki*, Gefährderkonzepte in der Kriminalpolitik, 155 ff.

[299] BVerfG NJW 2016, 1785; for more, see *Roggan*, NJW 2009, 257.

[300] On the scope of the so-called counterterrorism database, see *Roggan*, Die unmittelbare Nutzung geheimdienstlicher Informationen, 269–291; on the question of its constitutionality, see *Arzt*, NVwZ 2013, 1328 – 1332.

[301] On this, see § 2 Counter-Terrorism Database Law; § 2 Right Wing Extremism Database Law.

[302] Compare §§ 2 I Nr. 1, 3 II of Counter-Terrorism Database Law with §§129a, 129b StGB; § 2 I Nr. 2 Counter-Terrorism Database Law with §§ 89a, 89b, 89 c StGB; § 2 I Nr. 2 Counter-Terrorism Database Law with §§ 91, 111, 130, 130a, 131, 140 StGB.

[303] On this, see *Roggan*, NJW 2009, 258.

[304] *Sieber*, Der Paradigmenwechsel, 356.

[305] *Sieber*, Der Paradigmenwechsel, 356.

[306] For more, see *Abbe*, Der polizeiliche Staatsschutz und seine Datenbanken. [https://police-it.org/der-polizeiliche-staatsschutz-und-seine-datenbanken]; see also above III.A.2.d) Overlaps between Preventive and Repressive Police Investigations.

turning the department of state protection into a criminal intelligence service not covered under the law.[307] Moreover, the investigations by the criminal prosecution authorities may not be as effective as desired, both for the detection of potential suspects of certain serious crimes and for the difficult proof of their guilt at trial. Nevertheless, they can count on the support of the other security services, above all the intelligence services, which also operate in certain crime-related areas from the earliest possible point in time and without the requirement of a single specific incident, let alone the suspicion of a crime.[308] To ensure that nothing remains unknown about certain serious crimes, the areas of responsibility of the intelligence services are now matched with these crimes and the objective is to elevate the cooperation between the criminal prosecution authorities and the intelligence services to the highest level.[309] Further, to make sure that the level of information is the same for all players in the new security architecture, the information gathered is supposed to be disseminated in an institutionalized and consistent manner, for instance within the framework of a joint platform or collective databases.[310]

The measures of the new security law as outlined above are characterized by two specific features highlighted by the German Federal Constitutional Court: either they intervene *deeply* in the privacy of wide sections of the population or the entire population or they refer to specific case-dependent measures targeting individuals who have come to the attention of the authorities.[311] The constitutional readjustment of the protection of basic rights and freedoms, particularly by its demand for proportionality in infringements, forced the Court to depart from its longstanding jurisprudence holding that intelligence services and police authorities have *strictly* different responsibilities and powers and are consequently bound by *strictly* different thresholds.[312] This applies not only where intelligence services are given responsibilities and powers resembling conventional preventive police investigations but also where the police are asked to carry out so-called third-track duties that exceed the thresholds of concrete danger and reasonable suspicion, i.e. the precautionary prevention of danger (*Gefahrenabwehrvorsorge*) and the precautionary preparation of criminal prosecution (*Strafverfolgungsvorsorge*): the so-called prefield investigations of the police (*polizeiliche Vorfeldermittlungen*).[313]

---

307 German scholars describe this phenomenon as 'intelligencing of criminal prosecution' (Vergeheimdienstlichung der Strafverfolgung).

308 See above III.A.1. Intelligence Services.

309 *Lang*, Geheimdienstinformationen, 1 ff.

310 *Sieber*, Der Paradigmenwechsel, 360 ff.

311 BVerfG NJW 2016, 1784; see also BVerfG NJW 2006, 1941.

312 BVerfG NJW 2008, 831.

313 BVerfG NJW 2005, 2610; see also above III.A.2.c) Repressive Policing.

The Court emphasizes that these security measures, which are characterized by a lack of suspicion and by a wide range of targets, will principally constitute a serious infringement on the basic rights of those affected, as these individuals are unrelated to a concrete misconduct and nothing in the conduct of those affected caused the security authorities' response. These individuals are the more impacted in their basic rights the less they themselves have given cause for the state intervention.[314] In terms of intelligence law, it must be emphasized that the law does not include corresponding restrictions with regard to the targets of their information gathering investigations.[315] However, the issue of the balance between security and freedom or total surveillance and limited monitoring comes up again, especially in view of the huge increase in the technical capacity for information collection and processing.

With regard to preventive police action, the Court noted that the question of proportionality of an intervention in basic rights to prevent the threat of a future impairment of a legal interest as early as in the pre-field of a specific danger hinges not only on the prognosis of a reasonable prospect that the police action will succeed. It also depends on the degree of proximity which respective regulations require between the affected person and the anticipated endangerment of the legal interest in question. The lawmakers would ignore the constitutional limits if they granted the security authorities the power to seriously infringe basic rights and at the same time failed to stipulate requirements detailing the probability of ensuing danger and the proximity between the person and the danger in question.[316]

Following the overview on selected issues above, the reconfiguration of the security, intelligence, preventive police, and criminal prosecution laws will be detailed below in light of the corresponding jurisprudence of the Federal Constitutional Court on specific measures.

### 2. Precautionary Data Retention

The precautionary data retention regulations highlighted above are characterized by the fact that they authorize the intelligence services to receive personal data even in the conventional pre-field of information gathering; for instance, metadata storage is based on the assumption that telecommunication has an inherent specific potential for danger.[317] Metadata is stored without any cause or suspicion because the metadata of all citizens is stored, without reference to an attributable and objectionable behaviour, without any—not even an abstract—danger or any other quali-

---

[314] BVerfG NJW 2006, 1944; BVerfG NJW 2008, 1507 ff.

[315] See above III.A.1. Intelligence Services.

[316] BVerfG NJW 2006, 1946.

[317] BVerfG NJW 2010, 839.

fied situation. This type of data retention targets typical activities of daily life. And it is comprehensive, so that telecommunication users have no way whatsoever of avoiding it. There is no alternative means of communication without being registered.[318] Despite the gravity of the restrictions on the right to informational self-determination, the German Constitutional Court holds that the fact that, in Germany, telecommunication traffic metadata is stored as a precaution and without cause (*vorsorglich und anlasslos*) for a limited period of time in order to make them available to the intelligence services, the preventive police, and the criminal prosecution authorities is not per se illegitimate. According to the Court's jurisprudence, the retrieval and immediate use of metadata is proportionate for purposes of criminal prosecution if there are certain facts confirming the suspicion of a serious offence. In case of preventive police and intelligence investigations, proportionality will be maintained provided there are factual indications of a concrete danger for the limb, life, or freedom of a person, or for the existence or security of the federation or *Länder*. This means that the Court, on the one hand, requires a lower threshold for providing telecommunication metadata to the intelligence services. On the other hand, however, the Court establishes that the existence of a so-called 'common danger' (*gemeine Gefahr*) is sufficient for the retrieval and immediate use of this data by agencies involved in the prevention of danger at different levels, namely the preventive police and the intelligence services.[319]

As this jurisprudence of the Court implies, the constitution does not categorically prohibit the precautionary retention and storage of personal data but aims to protect against disproportionately designed data collection, in particular against unlimited objectives: the collection of precautionary and non-suspicion-based data is only permitted by exception. The foundation for and the design of data collection, particularly the objectives and conditions, are subject to strict requirements.[320] However, the possibility that the retention of metadata can be designed in conformity with the constitution cannot be taken to mean unlimited power for further regulations targeting the storage of all data conducive to the prosecution or prevention of crime. The constitution strictly prohibits the lawmaker from actually seeking to reconstruct all the activities of citizens, also by using already existing databases. It is an integral part of the constitutional identity of the Federal Republic of Germany that the all-round monitoring and recording of citizens in the exercise of their freedom is not allowed.[321] Similarly, in the words of the Court, 'the storage of personal data for purposes that are indefinite and not yet be determined [sic] is strictly pro-

---

318 BVerfG NJW 2010, 838.

319 BVerfG NJW 2010, 841 ff.; see also above III.A.1.c) Federal Office for the Protection of the Constitution (BfV) and III.A.2.b) Preventive Policing.

320 BVerfG NJW 2010, 838.

321 BVerfG NJW 2010, 839; see also BVerfGE 65, 1, 42 ff.; BVerfG NJW 2006, 980; BVerfG NJW 2006, 1943; BVerfG NJW 2008, 1509; BVerfG NJW 2012, 1425.

hibited.'[322] This means that the Court refuses to pursue a precaution-based security policy, which, as already highlighted above, aims to gather the following information or achieve the following objectives: how do people behave? What is the extent of associated risks as a result thereof? What risks are actually caused and might be averted? What are the possible causes or to whom or what can the risks be attributed?[323]

The Court found that the Data Retention Act (*TKÜ-Gesetz*) of 2010 failed to meet the requirements outlined above and declared it unconstitutional. Following the amendment in 2015, metadata may be stored from between four to ten weeks.[324] The Court has not yet addressed the Data Retention Act on the merits de nova.[325] Most recently, the Court requested an advisory opinion of the European Court of Justice.

### 3. At the Level of the Intelligence Services

#### *a) Federal Intelligence Service*

The realm of the intelligence services was also reconfigured. The responsibilities of the Federal Intelligence Service (BND) have been considerably expanded. Beginning in 1994, after the end of the Cold War and particularly after the attacks of 9/11, certain crimes such as terrorism; proliferation of weapons of war; illegal trade with goods, software, and technology; organized crime, i.e. drug trafficking, money laundering, illegal migration and counterfeiting; and cybercrime were declared relevant to Germany's security policy and as such subject to intelligence gathering.[326]

The BND's assignment to intelligence gathering on certain types of crime raises serious constitutional questions. First, it affects the constitutionally stipulated separation of competences between the federation and the *Länder*: the constitution assigns preventive and repressive law enforcement powers to the police authorities at the *Länder* level. As a federal body, the BND has no competence in this regard.[327] Second, even within the competences at the federal level, the specific competence

---

[322] BVerfG NJW 2012, 1423 f. (official translation by the Court https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2012/01/rs20120124_1bvr129905en.html); BVerfG NJW 2000, 57; already established by the landmark decision of the Federal Constitutional Court in BVerfGE 65, 1, 41 ff.

[323] For more see above I.B. Domestic Security as a 'Natural Problem to Solve'.

[324] § 113b TKÜ-Gesetz; see also the draft amendment Drucksache 18/5171, http://dip21.bundestag.de/dip21/btd/18/051/1805171.pdf.

[325] See also BVerfG Decision of 20 Dec. 2018 – 2 BvR 2377/16.

[326] § 5 I nos 1–10 Art. 10-Gesetz; see also BVerfG NJW 2000, 55 ff.; *Daun*, Die deutschen Nachrichtendienste, 69.

[327] See above III.A.1. a) Structure.

of the BND is intelligence gathering with regard to foreign security policy.[328] Thus, not all subject matters with a foreign connection come automatically under the constitutionally regulated jurisdiction of the BND.[329] Any intelligence gathering by the BND must relate to matters of foreign and security policy and to interests which the Federal Republic of Germany must maintain as part of the international community of states and its relations with intergovernmental institutions. The transnational nature of certain types of crime per se does not meet that material threshold; the BND's involvement may be justified if the recently introduced crimes also qualify in terms of security policy. According to the Federal Constitutional Court, this applies in cases of weapons/arms proliferation, arms trafficking, international terrorism, drug exports, and related money laundering, provided these activities are not only characterized by the fact that they are crimes but that they emanate from foreign states or organizations operating with the support of or by being tolerated by the foreign state. As such, they might assume proportions requiring international countermeasures. Thus, in the eyes of the Court, intelligence gathering by the BND on the above-referenced crimes is primarily relevant for purposes of foreign security policy. By consulting the government on these issues, the BND enables the government to adjust its foreign and security policy and its international cooperation with regard to security-related areas of crime.[330]

The fact that the German Federal Constitutional Court accepts the BND's involvement in the gathering of intelligence on certain types of crime also means that it accepts new emerging parallels and overlaps between the preventive and repressive policing duties. As long as the responsibilities and areas of activity of the different bodies defined by the distribution of competences are not commingled, the parallels and overlaps are acceptable under the constitution. The Court holds that there is no such commingling, first, because the BND is not explicitly tasked and equipped with powers to prevent, avert, or prosecute crimes as such. Second, the intelligence gathered with regard to certain transnational crimes is *primarily* used for purposes of the government's security policy.[331]

Another problem arises from the fact that the BND also uses standard intelligence techniques for information gathering on crimes of interest to Germany in terms of foreign security. Specifically, intelligence is gathered by strategic monitoring of certain types of crime without any suspicion (*verdachtlos*), affecting everyone indiscriminately. In return, targeting an individual's telecommunication lines is principally prohibited. The Court explicitly states that the BND's intelligence gath-

---

328 See above III.A.1. b) Federal Intelligence Service (BND).

329 BVerfG NJW 2000, 59; emphasized again BVerfG NJW 2013, 1502.

330 BVerfG NJW 2000, 60.

331 BVerfG NJW 2000, 60.

ering on certain types of crime would not pass the proportionality test without this restriction.[332]

The Court's above-mentioned reasonings have been the topic of controversial debate in the literature. The point about the relevance of foreign security for certain types of crime is not considered persuasive.[333] The creation of an overlap area called foreign security policy-related crimes and the provision of the BND with appropriate powers are viewed as support for criminal prosecutions by the BND.[334] At the centre of criticism are the intelligence gathering results on overlapping crimes. The criticism relates first and foremost to information gathered by the BND through strategic telecommunication monitoring under the G-10 Act. Even if the information thus gathered is primarily used by the government for national security purposes, the secondary use is clearly the support of other security authorities. In fact, the Act's objective is for the BND to transfer the intelligence so gathered to the authorities to promote the prevention, investigation, and prosecution of foreign security policy-related offences. A remarkable feature of the BND's activities in the new areas of observation is that they are quite operational in nature because their success depends on closer cooperation with other administrative bodies, including the criminal prosecution authorities.[335] Ultimately, the standard threshold for criminal prosecution, the so-called initial suspicion (*Anfangsverdacht*), is bypassed by strategic monitoring, which starts in the pre-field of any suspicion of a crime.[336]

Most recently, the BND's participation in the counterterrorism database once again raised the question of whether this amounts to a contravention of its constitutionally defined responsibilities.[337] The German Constitutional Court rejected the argument that the BND, by being assigned to the counterterrorism database, is subject to a 'further general task to prevent crimes of international terrorism'. The Court ruled that the BND's access to the counterterrorism database as well as the obligation to make its intelligence available to the other security authorities via the database cannot be viewed as *tasking* it with the *prevention* of international terrorism.[338] However, there is no denying that by participating in the counterterrorism database the BND will at least have an indirect influence on it.

A less controversial responsibility of the BND in the area of criminal prosecution is becoming more and more important: the investigation of crimes committed

---

[332] BVerfG NJW 2000, 63; § 5 II no 2 BND-Gesetz, however, makes an exception with regard to foreign telecommunication lines used by non-Germans.

[333] *Paeffgen*, StV 1999, 670, and 675.

[334] *Paeffgen*, StV 1999, 676.

[335] *Daun*, Die deutschen Nachrichtendienste, 69.

[336] *Paeffgen*, StV 2002, 337.

[337] BVerfG NJW 2013, 1502.

[338] BVerfG NJW 2013, 1502.

abroad and their investigations outside German territory and outside the jurisdiction of domestic criminal prosecution agencies.[339] The BND has recently been collecting information for the prosecution of foreign fighters who joined ISIS in Syria and, after its defeat, returned to Germany.

### *b) Federal Office for the Protection of the Constitution*

Not only the foreign intelligence service but also the domestic intelligence services at the *Länder* level have been given new crime-related tasks. Organized crime started to be considered a threat to German national security in the early 1990s. In order to facilitate the observation of this 'new threat', a number of domestic intelligence services at the *Länder* level were given information gathering powers.[340] It was argued that this expansion of powers is permitted because the principle of separation applies only between the federal intelligence services and the police authorities but does not apply at the *Länder* level. Hence it was suggested that the lawmakers at the *Länder* level may assign preventive and repressive police tasks to or may order closer cooperation with the domestic intelligence services. Moreover, it has been argued that the fight against organized crime by the domestic intelligence services can also be justified in light of their conventional responsibilities, namely the protection of the constitutional order against certain anti-constitutional political threats:[341] the important aspect in terms of security policy are the efforts by organized crime to diminish and paralyze the authority of the state in order to create 'areas outside state control and the law'.[342]

In addition to the new task of combating organized crime, domestic intelligence services were also given new terrorism-related powers.[343] These new counterterrorist powers are principally nothing more than the genuine responsibility of domestic intelligence services.[344] As a result, they do not raise fundamental questions.[345] In fact, terrorism is one overlap area between the intelligence services and criminal prosecution authorities. The connection between the BfV and the criminal prosecution authorities originates in the overlap area of the so-called politically motivated crimes. However, the recent counterterrorism law moved both areas closer

---

339 On this, see *Gusy*, § 1 BND-Gesetz, at 45 ff.; also BVerfG NJW 2000, 57 ff.; *Daun*, Die deutschen Nachrichtendienste, at 67.

340 *Daun*, Die deutschen Nachrichtendienste, 68.

341 BVerfG NJW 1971, 278; see for more above III.A.1.c) Federal Office for the Protection of the Constitution (BfV).

342 *Gusy*, § 1 BND-Gesetz, at 31; *Daun*, Die deutschen Nachrichtendienste, 68.

343 BVerfG NJW 2008, 828 ff.

344 See also above III.A.1.c) Federal Office for the Protection of the Constitution (BfV).

345 See also BVerfG NJW 2008, 828; *Rose-Stahl*, Recht der Nachrichtendienste, 75.

together.[346] Another new development is the growing intrusiveness of the information gathering powers of domestic intelligence services to the point of approaching conventional police investigation techniques, which, in the past, were only permitted under police law in case of concrete danger.[347]

As a result of its reorientation policy, the German Constitutional Court also does not oppose the legislature's restructuring of the security architecture. This means that the domestic intelligence services can broaden the objective of their observations and investigations to include the protection of conventional legal interests under police law provided the threat is the responsibility of the domestic intelligence services in a broad sense. This is the case with terrorism, which is not only anti-constitutional, and, as such, a legitimate intelligence gathering target[348] but also one with considerable potential for real harm. The domestic intelligence services may now address the prevention of terrorism-related harm, but in keeping with standards comparable to those already developed in police law. The Constitutional Court justifies this requirement by the fact that the investigative measure which domestic intelligence services intend to use in the context of danger resulting from terrorism—the secret infiltration of an information technology system (by means of a so-called 'state trojan')—entails, for the affected person, the same a degree of infringement on his or her basic rights[349] as a use based on police law. The Court also points out that the extent to which the investigation authority (the domestic intelligence services) reveals the personality of the affected person is significant.[350] Thus, the use of a 'state trojan' is considerably different from conventional intelligence gathering techniques of the intelligence services: it targets a certain individual in order to assess the dangerousness in terms of his or her intentions and capabilities to cause harm. As the intensity and objectives for using the 'state trojan' are comparable to preventive police investigations, the Court principally rejects the argument that the conditions for the domestic intelligence services to use this investigative measure should be less restrictive.[351] According to the Court, the proportionality test also requires the presence of a qualified danger and the use of 'state trojans' only for the protection of important legal interests on a case-by-case basis. In defining these conditions, the Court, on the one hand, permits the use of this investigative technique by the domestic intelligence services not only to protect the public interest in terms of the foundation or the continued existence of the state (including public utilities) but also to protect the life, limb, and freedom of the in-

---

346 *Roxin*/*Schünemann*, Strafverfahrensrecht, 63.

347 See above III.A.2.b) Preventive Policing.

348 See above III.A.1.c) Federal Office for the Protection of the Constitution (BfV).

349 The guarantee of confidentiality and integrity of information technology systems, according to Art. 2 I in conjunction with Art. 1 I Basic Law.

350 BVerfG NJW 2008, 832.

351 BVerfG NJW 2008, 832.

dividual.[352] The fact that these individual interests are included indicates a clear shift in the responsibilities of the domestic intelligence services towards those of the preventive police in the context of terrorism. On the other hand, the Court accepts that the standard threshold of preventive police law, namely the presence of a concrete danger, should be modified for the prevention of harm by the intelligence services: if it is not yet possible to establish with sufficient probability that a danger will turn to harm in the near future, the presence of a so-called 'impending' (*drohende*) danger suffices. 'Impending' danger means that certain facts lead to the conclusion that a certain threat exists, which can at least be identified and, by its nature, can be predicted in terms of time, and where certain persons can be sufficiently identified as a source of threat to allow taking surveillance measures specifically against them.[353] Thus, the Court introduces a modified version of the standard threshold of preventive police investigations, which clearly facilitates the limited surveillance of certain individuals and exposes them to the measures of preventive intelligence investigations in the pre-field of police law. Here, too, the Court relaxes the degree of proximity in time or closeness to future harm and considers efforts, plans, and pre-crime preparatory acts as sufficient. In fact, such an expansion of pre-field surveillance into the prevention of terrorist danger was more or less a conceptional necessity after some preparatory crimes had been introduced into the German Penal Code. As a result, domestic intelligence services were no longer in a position to ensure the prevention of preparation in the context of terrorism with the conventional 'concrete danger' standard, which requires greater proximity in time or closeness to future harm.[354]

### 4. At the Level of the Police

#### *a) In general*

The reorientation also resulted in changes at the level of police law. The most fundamental change in recent decades was to assign the police to so-called third-track duties, i.e. duties beyond the thresholds of concrete danger and reasonable

---

[352] BVerfG NJW 2008, 831.

[353] BVerfG NJW 2008, 831; compare the definition of danger in case of residential surveillance conducted by Federal Criminal Police Office in BVerfG NJW 2016, 1784. As this measure also constitutes a serious interference with the right to privacy, the Federal Constitutional Court considers the imposition of this measure only proportionate if it is directed against a person who is implicated in a possible violation of the law from the perspective of a reasonable third party, where the protection of high-ranking legal interests, in particular life, limb, personal freedom, as well as the existence and security of the federation or *Länder* are at stake and where these must be protected against an offence of significant gravity.

[354] See also the difficulty to base a precautionary interception on the 'planning stage' of endangerment and preparation offences, BVerfG NJW 2004, 2217.

suspicion, namely the precautionary prevention of dangers (*Gefahrenabwehrvorsorge*) and the precautionary preparation of criminal prosecution (*Strafverfolgungsvorsorge*).[355] In both cases precaution is not based on factual circumstances of individual danger or a certain suspicion regarding a specific crime. Thus, questions were raised not only whether such an expansion can be permitted in the first place but also how, in both cases, precaution can be limited, as the idea of precaution itself comes with the potential to justify unlimited investigations.[356]

The question of the constitutionality of precautionary preparations for future criminal proceedings had to be addressed not only from the perspective of proportionality because the corresponding measures include significant interventions in the right of affected persons to informational self-determination; it also had to be raised due to the fact that individual *Länder*, not the federal legislature, were introducing this new task into their police codes, including investigative powers for their police agencies. As highlighted in the German Constitutional Court's respective jurisprudence, these regulations in the police codes of the *Länder* created the problem that the *Länder* police authorities were in a position to apply, for purposes of criminal proceedings, the police law of their *Länder* in addition to the Federal CCP. For instance, for purposes of evidence gathering the police were authorized to bypass the Federal CCP and to conduct wiretappings based on their *Länder* code, contrary to federal law, even in the pre-field of certain preparatory acts, an attempt, or the execution of a specific crime. The Court established that the constitution could hardly allow the police to apply two different standards for purposes of criminal prosecution, thereby creating contradictory concepts of administering criminal justice. Therefore, the competence of the federal legislature to regulate the 'court trial' enshrined in Art. 74 I No. 1 Basic Law must be understood as exhaustive in terms of all future or current criminal prosecutions.[357]

As regards the effects of measures of precautionary preparations for the future prevention of dangers and future criminal proceedings, the German Constitutional Court found that introducing corresponding police powers aimed at precaution is in both instances not *per se* unconstitutional, even if the question of a reasonable limitation of prosecutorial powers remains to be answered and does not appear easy compared with 'concrete danger' and 'suspicion'.[358]

In the following, we will present in more detail the Court's jurisprudence on selected investigative measures under preventive police law.

---

355 For more see *Roggan*, NJW 2009, 257.

356 BVerfG NJW 2004, 2216; BVerfG NJW 2005, 2607; see also above II.A.3. Position of the German Federal Constitutional Court.

357 BVerfG NJW 2005, 2607.

358 BVerfG NJW 2004, 2216; BVerfG NJW 2005, 2607.

*b) Precautionary wiretapping in the pre-field of concrete danger*

In its decision on the interception of telecommunications by the police of Lower Saxony, the Court found the state's provision in its Code for Public Order and Security unconstitutional. The provision had authorized the police to wiretap the telecommunications of persons provided there are facts justifying the assumption that they will commit serious crimes and provided there is no other way to secure the precautionary prevention or the precautionary preparation of the prosecution of such crimes. At the centre of the constitutional review was the lack of clarity in the reason for the wiretap. Thus, the Court did not categorically reject tasking the police with preventive duties, beginning as early as in the pre-field of a concrete danger of committing a crime. Nevertheless, pre-field investigations by the preventive police must be further defined, *inter alia* in terms of specific acts by individuals that could justify preemptive police intervention. The fact that the police are empowered to interfere with the basic rights and freedoms in the event of any potentially relevant act by an individual that might lead to a crime is not only equivalent to unlimited empowerment, but it also entitles the police to balance freedom with security on a case-by-case basis. The latter power requires legislative regulation.[359]

In its second decision on the interception of telecommunications by the Federal Customs Criminal Investigation Office for purposes of the precautionary prevention of future crime,[360] the Court again objected on the grounds of lack of clarity of the federal preventive law: as the pre-field of a concrete danger consists mainly of activities of daily life, which are unlikely to cause harm, the precaution-based police power must be framed in a way that provides restrictive elements for corresponding police actions and introduces standards of predictability and controllability comparable with the conventional thresholds of police prevention and prosecution.[361]

The pertinent provision of the Foreign Trade and Payments Act allowed the Customs Criminal Investigation Office to intercept telecommunications provided there were facts justifying the assumption that certain persons were planning to commit certain serious offences specified by reference to corresponding provisions. The Court found that this provision lacks clarity, first, because it fails to define the scope of offences to be prevented by precautionary interception due to the complicated reference technique the legislature had employed in the provision. Second,

---

[359] BVerfG NJW 2005, 2608.

[360] For more on the preventive and repressive investigations by the Customs Criminal Police Office, which has become increasingly important regarding the prevention and investigation of crimes in cross-border trade with goods and services important in terms of security: smuggling of weapons, export control of armament and dual-use goods, combating organized crime and international terrorism, see *Daun*, Die deutschen Nachrichtendienste, 70.

[361] BVerfG NJW 2004, 2216; BVerfG NJW 2005, 2607.

the 'planning' requirement, being only a temporal condition of the interception threshold, does not minimize the risk of a false prognosis, so that the interception could have been considered tolerable. As the Court highlights, 'planning' can be broadly understood to the extent that the Customs Criminal Investigation Police must consider even the inner thoughts (*forum internum*) of potential offenders in order to justify 'its assumption', as in most cases 'planning' is not carried out in the form of a single act.[362] In fact, the reference to some offences that should be prevented by precautionary interception is not at all conducive to specifying the 'planning stage' as a threshold because, at that stage, the circumstances presumably leading to the commission of certain crimes do not provide reliable corresponding indicators. In terms of the facts involved in 'planning', a reliable prognosis on whether the person in question may commit exactly the offences covered under the Act is not possible. Further, the possibility that some actions perceived as 'planning' may end up being completely harmless is quite high, given some of the endangerment and preparation offences in the Foreign Trade and Payments Act: these crimes are basically committed by merely behaving in a certain way. They are not carried out in distinct stages in terms of time and action, such as planning, preparation, attempt, execution, etc. Compared to offences with such distinct stages, the planning of a certain objectionable behaviour under the Foreign Trade and Payments Act cannot be clearly distinguished from entirely unobjectionable behaviours. For these reasons, the Court found the respective provision of the Foreign Trade and Payments Act unconstitutional.[363]

### *c) Precautionary screening in the pre-field of concrete danger*

Another example of precaution-based preventive police law lacking clarity was the police law of North Rhine Westphalia. The former § 31 North Rhine Westphalian Police Code authorized the police to conduct comprehensive computer-assisted screenings in order to identify so-called sleepers (*Schläfer*). Sleepers are individuals presumably prepared to carry out terrorist attacks but who present themselves as ordinary, fully adjusted citizens, whose conduct is inconspicuous. The Code authorized the preventive police to 'require public bodies and entities outside the public sector to transfer personal data of certain groups of persons from their databases for the purpose of automatic matching with other databases, to the extent necessary to prevent a current danger to the existence or security of the Federation or of a

---

362 BVerfG NJW 2004, 2217.

363 BVerfG NJW 2004, 2217; at the same time, the Court accepts that in case of a precautionary interception of telecommunication, the assumption, even it is based on factual circumstances and must not be merely presumption, might include general experiences of the police gained from previous investigations in similar cases. In fact, this is a further reduction with regard to the factual basis of a prognosis made by preventive police; see in this regard above III.A.2.b) Preventive Policing.

Land or for the body, life or freedom of a person (dragnet)'. The scope of personal data was 'limited to the name, address, date and place of birth as well as other data required for an individual case; it may not extend to personal data subject to professional protection or officially sensitive information'.[364]

The dragnet-related investigative power of the Westphalian police was characterized not only by its wide range with regard to affected persons but also by the fact that these persons were not suspected of posing a danger. As the German Constitutional Court highlighted, police screenings usually evaluate general circumstances—see the example in footnote 365—which usually cannot substantiate any suspicion of a behaviour that is even potentially disturbing or endangering. The actual purpose of the screening in the instant case was to reduce the circle of individuals who might be the subject of further investigations, which will eventually provide factual reasons for justifying a suspicion. As such, the screening was clearly aimed at 'extracting suspicion' (*Verdachtsgewinnung*). In fact, the screening generally resembles the strategic monitoring by the intelligence services insofar as it also indiscriminately targets a wide range of persons without any suspicion. As such it operates in the pre-field of the conventional threshold of preventive policing, which principally requires a substantiated suspicion of danger and the person in question as responsible disturber.[365] Given that both proportionality factors were not satisfied, the preventive police screening was a serious infringement on the basic right to informational self-determination. Still, the German Constitutional Court found the screening not disproportionate and unconstitutional *per se*. The Court argued that there were high-ranking constitutional interests weighing on the side of public interest: the existence or security of the federation, of a *Land*, or of the body, life, or freedom of a person. The Court emphasized that these constitutionally protected interests are threatened by terrorist aspirations, which the state must effectively address.[366] Thus, the conventional standard of preventive police law—the affected person's behaviour must exhibit a certain degree of closeness to the anticipated future harm and be sufficiently substantiated by facts—cannot be met here. Nevertheless, the proportionality of preventive police screening can be guaranteed by requiring the existence of a qualified danger for the aforementioned high-ranking constitutional interests in order to exclude unlimited screenings. Moreover, the Court held that this danger need not be a present danger (*gegenwärtig*) as required by the Westphalian code but that a concrete danger, which requires a lower level of

---

[364] In the course of implementing said computer-assisted screening actions, the security authorities, the Westphalian police, demanded personal information on, for instance, the following matching terms: male, age 18 to 40 years, student or former student, Islamic religious affiliation, country of birth, or nationality of certain individually designated countries with predominantly Islamic populations.

[365] See above III.A.2.b) Preventive Policing.

[366] BVerfG NJW 2006, 1945.

danger, suffices. In addition, a concrete danger may also be permanent, which includes the prognosis of a harm occurring over a long period of time. However, the Court clearly stated that after 9/11 a general threat of a terrorist attack or a threat based on tensions on the international stage is not sufficient to justify a concrete permanent danger for purposes of preventive police screening.[367] Rather, the danger must have been substantiated so that the specific criteria used in the screening can identify a certain group of persons and further measures can be taken against them in efforts to prevent future harm.[368]

#### *d) Precautionary automatic licence plate recognition in the pre-field of concrete danger*

Not only grave interferences such as the interception or screening of telecommunications for purposes of preventive police investigation were subject to review by the Constitutional Court but also the automatic licence plate recognition (*automatische Kennzeichenerfassung*), which, according to the Court, is no less capable of profiling and interference with the right to informational self-determination.[369] The pertinent Hessian code of public security and order had authorized the police to use the automatic licence plate recognition system for purposes of matching it with the police database. This resulted in a virtually unlimited use of the automatic licence plate recognition system, applying it to any situation that could give rise to a reasonable probability of an anticipated future endangerment or impairment of a public interest. For instance, the simple presence at a particular location such as driving in an area close to the federal border or staying in a crime hotspot was sufficient for registration by the system.[370] The contested provision failed not only to mention a specific reason for the protection of a public interest but lacked any limits with regard to the vehicle drivers who might be subject to the automatic licence plate recognition system. The Court was struck by the fact that the provisions indiscriminately targeted persons who passed by the location where the system was set up. The Hessian legislature did not consider whether or not the individuals' behaviour provided a reason for being registered by the system.[371] Finally, the provision failed to define any objective for the registration. The phrase 'matching with the police database' was ambiguous and did not exclude the possibility of using the resulting 'hits' to create movement profiles of certain persons for purposes of preventive surveillance by the police.[372] Most recently the Court also declared uncon-

---

367 BVerfG NJW 2006, 1947.
368 BVerfG NJW 2006, 1948.
369 BVerfG NJW 2008, 1507.
370 BVerfG NJW 2008, 1516.
371 BVerfG NJW 2008, 1516.
372 BVerfG NJW 2008, 1510.

stitutional two laws by the *Länder* of Hesse and Baden-Württemberg on precautionary automatic licence plate recognition, *inter alia* for failing to meet the aforementioned requirements.[373]

## C. Main Concerns

The above-outlined reconfiguration of selected security issues reinforced the question about the boundaries between intelligence, prevention, and criminal prosecution. In the past, parallel intelligence investigations in the area of national security crimes were considered a necessity. Following the expansion of the responsibilities of the intelligence services to include certain crimes, there has been a noticeable trend of tasking the German services with 'criminal intelligence gathering'. Some even argue that to the extent that the functional separation between security branches is disappearing[374] as a result of overlapping responsibilities and commonly used investigative measures, overlapping jurisdiction may increase the competition between the services and the police.[375] The separation question is also raised with regard to the sharing of information between the intelligence services, the police, and the criminal prosecution authorities. The way in which the intelligence services typically consulted the police in the past, namely by providing reports about the general security situation, has been replaced by routine information sharing. Three features of this new way of information sharing have been pointed out: it covers more areas, it is deeper (in the sense of a more specific and case-based information transfer), and it is faster.[376] These developments not only increase the dependence of the police and criminal prosecution authorities on intelligence and provide the intelligence services a certain degree of power over these areas, but they also lead to the creation of information sharing mechanisms and a new way of thinking and acting that combines all resources and experiences to combat certain criminal phenomena.[377] More on the exact scope of information sharing between the intelligence services and the criminal prosecution agencies will follow below.

With regard to law enforcement, the tension between repressive criminal law, which is the domain of federal jurisdiction, and preventive police law, which is mostly that of the *Länder*, originates in the common legal interests both areas aim to protect regardless of what triggers the obligation to protect and how the protec-

---

373 BVerfG Decision of 18 Dec. 2018 – 1 BvR 2795/09.

374 *Gusy*, KritV 1994, 245; *Singer*, Die Kriminalpolizei 2006, 87.

375 *Zoller*, Rahmenbedingungen nachrichtendienstlicher Informationsgewinnung, 14; *Gusy*, KritV 1994, 245.

376 *Albert*, Informationsverarbeitung durch Nachrichtendienste, 105 ff.

377 *Albert*, Informationsverarbeitung durch Nachrichtendienste, 106.

tion is provided. Whereas criminal law provides the protection of individual or public legal interests by criminalizing certain acts constituting offences in specific provisions of the Penal Code or other criminal codes, police law protects the same legal interests in a rather unspecific manner by using the broad concepts of precaution or prevention of danger against these legal interests. As recent developments in the area of prevention demonstrated, the *Länder* use their jurisdiction for regulating prevention extensively and therefore compete with the federal criminal justice system. The most recent introduction of indefinite preventive detention in Bavaria is just one example of how preventive police law can compete with criminal law.[378] Meanwhile preventive police law has incorporated almost all coercive and secret measures which the CCP provides for criminal investigation. The forum shopping of the police in case of so-called measures with a double function justifies the claim that criminal procedure law has been undermined by preventive police law.[379]

In fact, as detailed above,[380] there is no denying that there is also some degree of overlap between preventive and repressive police investigations: in case of crime, prevention is needed as long as the criminal offence has not been completed yet. More specifically, prevention may overlap with criminal prosecution in scenarios where the perpetrator has already left the 'planning' stage, entered into the commission of a crime, and the legal harm continues, as the crime is not completed.[381] Compared with criminal prosecution, the preventive duty of law enforcement applies in any event in the pre-field of a punishable form of a punishable act. These explanations indicate that not only the definition of concrete danger but also the conventional distinction between preventive and repressive police actions are mainly based on the features of an offence that consists of a set of acts and a harmful result (*Erfolgsdelikte*, result crime) or is committed over a period of time (*Dauerdelikte*, continuing offence), especially within an organization.[382] The concept of concrete or abstract endangerment offences, mostly in form of a single act, as well as the expansion of organizational offences certainly extended the scope of human behaviour and of matters potentially subject to preventive police measures.

---

[378] § 20 para 3 Bavarian Police Law; see also Brodowski, Alternative Enforcement Mechanisms, 389 f.; Engelhart, Countering Terrorism, 459.

[379] Meyer-Goßner/*Schmitt*, § 163 (StPO) at 17; *Gusy,* Polizei- und Ordnungsrecht, 8.

[380] III.A.2.d) Overlaps between Preventive and Repressive Police Investigations.

[381] BVerfG NJW 2004, 2217.

[382] *Gusy,* Polizei- und Ordnungsrecht, 12.

# IV. Intelligence Information in Criminal Proceedings

## A. Securitization of criminal proceedings

When the German Code of Criminal Procedure was introduced in 1879, the open collection of evidence was the rule. Secret measures (e.g. secret observations by the police) were rare exceptions. This situation changed dramatically in the 20th and 21th century, especially with the ongoing development of new technological (surveillance and information gathering) measures and the growing use of informants or undercover agents in certain areas of serious crime.[383] Today, the use of secret measures in criminal investigations is more often the rule than the exception, at least in some areas. Moreover, as mentioned above, not just the police and prosecution play a major role in gathering secret evidence in certain areas of serious crime but the intelligence services do so as well.[384] Particularly the fact that the intelligence services were tasked with combating major crime, especially transnational crime, resulted in a cooperation with and increased intelligence transfer from the foreign intelligence services.[385] In addition, the German foreign intelligence service (BND) is the main supplier of evidence with regard to crimes committed abroad and subject to jurisdiction of German courts. More recently, the BND collected evidence for criminal investigations against those foreign fighters who joined ISIS or other terrorist organizations in Syria but subsequently returned to Germany.

Both the growing use of secret investigative techniques by criminal prosecution authorities and the growing interaction between intelligence services, police, and prosecution give rise to conflicts with established principles of criminal procedure, rights of defence, and the constitutionally guaranteed protection of informational self-determination.[386] From the perspective of criminal procedure law the conflict is most obvious where police and intelligence authorities do not allow the unrestricted use of their investigative results in criminal trial, inter alia with reference to the protection of state secrets.[387] Similarly, the sharing of information between different branches of the security apparatus raises the question whether or to what extent a transfer of intelligence information to the criminal prosecution agen-

---

383 For more, see *Hefendehl*, GA 2011, 209 ff.; *Schünemann*, ZStW 119/2007, 945–958; *Soiné*, Aufklärung der Organisierten Kriminalität, 12 ff.

384 *Engelhart*, The Secret Service's Influence, 505; for more see *Hefendehl*, GA 2011, 212 ff.; *Gusy*, KritV 1994, 242–251; *Denninger*, KritV 1994, 232–241.

385 *Vogel*, ZIS 1/2017, 28; for more see *Gercke*, CR 11/2013, 750; *Gnüchtel*, NVwZ 2016, 1113.

386 See also *Engelhart*, The Secret Service's Influence, 506.

387 See below IV.B.3. Suspending a Transfer and IV.C.2a) General Framework.

cies can be justified, as the original information gathering was conducted for other purposes.[388]

Legal systems generally provide strategies, on the one hand, to protect the public interest by restricting the disclosure of evidence in criminal proceedings and, on the other hand, to comply with procedural guarantees. First, German law also offers the possibility to withhold evidence classified as a state secret and to prevent its consideration by the trial court in the first place. This may be called 'non-disclosure'.[389] Second, some evidence may only be used at the investigation stage by the public prosecutor's office or the police and may never make it into the official case file. Certain intelligence information in particular may only serve as a tip or lead and be used as an indicator for further investigations or the criminal prosecution authorities may keep it entirely concealed from the court or the defendant. The latter is especially the case if the intelligence services only consent to a transfer of information provided it is not used as evidence in trial.[390] Third, and most importantly, intelligence information can be introduced into criminal proceedings as 'indirect evidence'.[391] Fourth, there are some other secondary protection techniques to ensure the protection of state secrets in criminal proceedings, notably restrictions on the right of access to the case file,[392] on the publicity of the main hearing,[393] and on the publicity of the verdict.[394] These secondary protection techniques will not be covered here for reasons of space.

To consider the above-mentioned strategies normatively, we shall first address the transfer and use of intelligence information at the investigation stage (B.) This includes not only the constitutional requirements for the protection of the right to informational self-determination and provisions of intelligence law but also the framework for the criminal prosecution authorities on how to use the transferred information. Particularly the above-mentioned strategy of using intelligence information as an 'investigative tip' will be explained in detail. Second, the use of

---

388 *Engelhart*, The Secret Service's Influence, 527; for more see below IV.B.2. Intelligence Information as Evidence at the Criminal Investigation Stage.

389 For more, see below IV.B.3. Suspending a Transfer and IV.C.2a) General Framework.

390 For more, see *Lang*, Geheimdienstinformationen, 130.

391 See below IV.C.2. Protection of State Secrets in Court Trial.

392 For the constitutional requirements in this regard, see BVerfG NStZ-RR 2013, 379–380; BVerfG NJW 1983, 1043–1046; see also BVerfG NJW 1984, 1451–1452; Frisch, Schutz staatlicher Geheimnisse, 204.

393 For more, see BverfG MMR 2017, 742; BVerfG GRUR 2016, 314; NJW 2012, 1865; BGH NJW 2006, 1221; see also Franke, NJW 2016, 2619; see also Fromm, NJOZ 2015, 1193.

394 For the constitutional requirements in this regard, see BVerfG GRUR 2016, 313–315.

intelligence information and the protection of state secrets at the trial stage will be explored (C). More specifically, we will provide a general overview of the main principles of a court trial in order to illustrate the tension between the use of intelligence and the protection of state secrets on the one hand and the interests of justice and the rights of defence on the other. We will also detail the solutions provided under German law.

## B. Transfer and use of intelligence information at the investigation stage

The Basic Law has considerable influence on German criminal procedure law. This is manifested not only in the constitutional principles that apply to the criminal investigation and court trial but also in the strong protection of the defendant's basic rights at both stages of criminal proceedings.[395] However, as the jurisprudence of the Federal Constitutional Court emphasizes, there are many cases where the legislature has the duty and a certain discretion to specify the constitutionally based principles of criminal proceedings and rights of defence.[396] The European Convention of Human Rights also contributes to a broad interpretation of defence rights. German criminal procedure law is further influenced by the case law of the European Court of Human Rights (ECtHR), particularly regarding the examination of witnesses.[397] This also applies where witness evidence is withheld on grounds of protection of state secrets.[398]

### 1. Main Principles of Criminal Investigation

According to the conventional concept of law enforcement responsibilities, the police serve either preventive or repressive functions.[399] Police authorities and police officers tasked with the prevention of danger are at the same time obligated under the Federal CCP to investigate on grounds of criminal suspicion.[400] Finally, the police also assist in the criminal prosecution, under the supervision of the pub-

---

[395] For more, see below IV.C.1. Trial Procedures and Main Principles and IV.C.1.b) Rights of defence.

[396] See for instance BVerfG NJW 1981, 1722; BVerfG NJW 1992, 2811.

[397] For the influences by the ECtHR in general, see, *Vogel*, The Core Legal Concepts and Principles, 42; see also BVerfG NJW 2007, 205; BGH NStZ 2017, 602 ff.; BGH NJW 2010, 2451; BGH, Decision of Jan. 27, 2015, Case no: 1 StR 396/04, BeckRS 2005, 02845.

[398] See below IV.C.2.b) Witness protection measures.

[399] *Graulich*, NVwZ 2014, 685; doubting that such a distinction in police practice is even possible, *Rzepka*, KritV 1999, 313.

[400] § 163 para 1; *Gusy*, Polizei- und Ordnungsrecht, 76.

lic prosecutor's office. As long as they carry out criminal investigation responsibilities, the police are subordinate to the public prosecutor and must follow and carry out his or her instructions.[401] However, as already mentioned above, in legal practice, it is typically the police who initiate the investigation, collect evidence, and present the results of the investigation to the public prosecutor in charge. Although it is officially the latter who leads the investigation, he or she determines the course of investigation and intervenes only in the more important cases.[402]

As mentioned, the police are obligated to 'take action in relation to all prosecutable criminal offences, provided there are sufficient factual indications'.[403] This requirement is the very foundation for the justification and obligation to investigate (the so-called initial suspicion) and must be based on specific circumstances.[404] The police may obtain said indication from reports by the victim, witnesses, other public institutions, from public or open sources (news or social media), and may come across respective circumstances in the course of their own actions unrelated to the specific suspicion.[405] The category of other public institutions also includes the intelligence services as they may voluntarily transfer information to the public prosecutor's offices or the police (for more explanations, see below).[406]

The German CCP provides a broad spectrum of investigative measures the police can utilize to verify the truthfulness of the suspicion against an individual.[407] It also provides a general clause that entitles the police 'to request information from all authorities and to make investigations of any kind, […] provided there are no other statutory provisions specifically regulating their powers'.[408] This includes the intelligence services, which the criminal prosecution authorities might call on for information by formal request (for more explanations, see also below).[409]

---

401 § 152 I of Courts Constitution Act (Gerichtsverfassungsgesetz); Meyer-Goßner/*Schmitt*, § 153 (GVG) at 1; *Roxin*/*Schünemann*, Strafverfahrensrecht, 60; *Vogel*, The Core Legal Concepts and Principles, 55.

402 *Roxin*/*Schünemann*, Strafverfahrensrecht, 61; Graulich, NVwZ 2014, 687; *Vogel*, The Core Legal Concepts and Principles, 56.

403 § 152 para 1; *Vogel*, The Core Legal Concepts and Principles, 55; BVerfG NJW 1984, 1451; *Engelhart*, The Secret Service's Influence, 525; *Greßmann*, Nachrichtendienste und Strafverfolgung, 403.

404 Meyer-Goßner/*Schmitt*, supra note 401, § 152 (StPO) at 4; *Gleß*, Predictive policing, 173 f.; *Kröpil*, JuS 2015, 213.

405 See § 160 para 1 German CCP; *Gusy,* Polizei- und Ordnungsrecht, 76; *Kröpil*, JuS 2015, 213.

406 See below IV.B.2.b) Unsolicited information transfer.

407 §§ 48 ff. StPO.

408 § 160 para 1 StPO; see also BVerfG NJW 1981, 1973.

409 See below IV.B.2.c) Transfer on request.

According to the principle of objectivity and the search for the material truth, public prosecutors are obligated to 'ascertain not only incriminating but also exonerating circumstances'.[410] Thus, the intelligence information might be relevant for the criminal investigation authorities on both counts. Unlike in the main trial, the principle of publicity does not apply at the investigation stage.[411] This stage is confidential as a matter of principle.[412] Although defendants have the right to access investigation files[413] already at the investigation stage, which ensures the constitutionally mandated respect for the defendant's dignity, i.e. not to be treated as a mere object of investigation,[414] this right is not absolute and can be restricted, *inter alia* to ensure an effective investigation or to protect state secrets.[415] As a result, most defendants will only be informed that there is some inculpatory evidence against them but not that the evidence originates in an intelligence investigation. In this way, intelligence information will be used as 'indirect evidence' against the defendant as early as the investigation stage.

Finally, the criminal prosecution is guided *inter alia* by the principle of mandatory prosecution.[416] This means not only that the police and the public prosecutor are compelled to investigate given 'sufficient factual indications', but also that the prosecutor must bring a public charge as a matter of principle if the outcome of preliminary investigations provides 'sufficient reason' for it.[417] The prosecution authority must be in a position to name and disclose all evidentiary material on which its allegations against the defendant are based.[418] This includes intelligence information used by the public prosecutor's office to support the indictment.[419]

---

410 § 160 para 2 StPO; BVerfG NJW 1983, 1043; for more see *Kröpil*, JuS 2015, 241.

411 Compare § 169 GVG.

412 BVerfG NJW 1984, 1451 – 1452, 1451 f.; Franke, NJW 2016, 2618.

413 § 147 para 2 StPO; BVerfG NJW 1984, 1451–1452.

414 BVerfG NJW 1984, 1452.

415 § 147 para 2 StPO; BVerfG NStZ-RR 2013, 379–380 (search warrant based on undisclosed evidence); BVerfG NJW 1984, 1451–1452.

416 *Arslan*, Aussagefreiheit des Beschuldigten, 196.

417 §§ 152 para 2, 170 para 1 StPO; see also *Roxin*/*Schünemann*, Strafverfahrensrecht, 79; Brandt, Bundesamt für Verfassungsschutz, 67 ff.; arguing that in police *practice* the principle of facultative investigation applies because prosecutorial oversight is quite limited, *Rzepka*, KritV 1999, 315; moreover, the principle of mandatory prosecution does not apply strictly. It is generally accepted that, given certain circumstances, the principle of proportionality might require dropping a criminal prosecution, conditionally or unconditionally; for more see *Vogel*, The Core Legal Concepts and Principles, 56.

418 See §§ 199 para 2 and 200 para 1 StPO; see for more BVerfG NJW 1983, 1043–1046; LG Hannover FD-StrafR 2015, 369880; MüKO/StPO-*Hauschild*, § 96 StPO, at 11.

419 Compare BVerfG NJW 1983, 1044.

## 2. Intelligence Information as Evidence at the Criminal Investigation Stage

### *a) General framework*

Intelligence information as evidence at the investigation stage is not only a matter of criminal procedure law but is also regulated by intelligence law. Thus, both laws apply simultaneously if the information is to be transmitted from the intelligence services to the criminal prosecution authorities. Problems arise if secretly gathered evidence, in whole or in part, is not to be used for criminal investigation purposes or at trial, as will be shown in more detail below; further, the transfer of or request for information as such also requires a legal ground and, most importantly, a justification. The Federal Constitutional Court considers the transfer, request, or use of personal data and information to or by other authorities, especially for purposes other than the one the data or information were collected for, as an infringement on the right to informational self-determination. Hence there must be a parliamentary provision allowing the transfer, request, or use in due consideration of the principle of proportionality. These are the basic requirements of the data protection law with regard to the transfer, request, and use of intelligence information for criminal investigations.[420] Further, as mentioned above, the German Federal Constitutional Court emphasizes that information sharing between the intelligence services and the police authorities is not permitted as a matter of principle. Departures from this principle are only permitted by exception and will generally constitute a serious infringement.[421]

The statutory framework of German foreign and domestic intelligence services regulating the sharing of intelligence information with other public authorities including the police and criminal prosecution authorities is quite fragmented. Not all services have specific regulations for the transfer of information in their own codes; furthermore, the transfer of some information, such as information gathered by telecommunication surveillance, is regulated separately. In view of the detailed and diverse regulatory framework, we will explain in the following the key features of the legislation relating to information transfer and will attempt to avoid further confusion by withholding specific references to the rather complicated regulation technique in this area. Moreover, information transfer provisions distinguish primarily between information sharing for purposes of prevention of crime and prosecution

---

[420] BVerfGE 65, 1 ff.; see also *Engelhart*, The Secret Service's Influence, at 517; *Sieber*, NJW 2008, 882; *Greßmann*, Nachrichtendienste und Strafverfolgung, 405; *Lang*, Geheimdienstinformationen, 104 f.; for further internal regulations between the intelligence services which cannot override statutory law, see *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 290; for the legal situation in the past, see *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 292 f.; for the requirements of the principle of proportionality, see *Arslan*, Intelligence and Crime Control, 510 f.

[421] BVerfG NJW 2013, 1505.

of crime.[422] As in most cases the same police authority is in charge both for prevention and prosecution, it is worth noting that the police authorities may receive relevant intelligence information at a fairly early stage where the preventive nature of the work by the authorities in charge is quite general or where a certain crime is only in the planning stage and has not necessarily been attempted or committed. Our focus, however, will be on information sharing for repressive purposes; information transfer for preventive purposes (in a broad sense) will not be addressed.

In general terms, the pertinent statutory framework contains two models of communicating intelligence information to the criminal prosecution authorities: the spontaneous or autonomous transfer by the intelligence services themselves[423] and the transfer on request by the criminal prosecution authorities.[424] The law further distinguishes between cases where the intelligence services are obligated to transfer relevant information and others where information sharing is at their discretion and where they are entitled to withhold relevant or requested information.[425]

The following explanations on the transfer of intelligence information to the police and criminal prosecution authorities do not claim to be exclusive; first, because this publication aims at providing a general overview of the respective frameworks and second, because some questions have still not been settled in the jurisprudence and are quite controversial among scholars. Further, the transfer of information by the German Financial Intelligence Unit to the criminal prosecution authorities will not be addressed either, as the Unit has a *sui generis* position in the German landscape of intelligence services and is based on a framework quite independent of conventional intelligence law.[426] Nor will the Act on Joint Databases regarding the security authorities, including the intelligence services and the criminal prosecution agency, be explored.[427] Finally, this book will also limit itself in that only the law of the federal intelligence services will be explored.[428] The federal intelligence ser-

---

[422] See for instance §§ 19 para 2 nos 1–4, 20 para 1 BVerfSch-Gesetz; §§ 4 para 4 nos 1 and 2, 7 para 4 nos 1 and 2 G10-Gesetz; for more see *Greßmann*, Nachrichtendienste und Strafverfolgung, 402; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 286 ff.

[423] §§ 19, 20 BVerfSch-Gesetz; § 24 BND-Gesetz; § 11 MAD-Gesetz; for more, see *Greßmann*, Nachrichtendienste und Strafverfolgung, 406 ff.

[424] § 20 para 2 BVerfSch-Gesetz.

[425] §§ 23, 24 BVerfSch-Gesetz; § 31 BND-Gesetz; § 12 MAD-Gesetz; for more, see *Greßmann*, Nachrichtendienste und Strafverfolgung, 408.

[426] See in general *Hütwohl*, ZIS 11/2017, 680 –687.

[427] For the joint databases of the intelligence services, criminal prosecution authorities, and police see Engelhart, The Secret Service's Influence, 521 ff.; for the scope of the so-called counterterrorism database, see *Roggan*, Die unmittelbare Nutzung geheimdienstlicher Informationen, 269–291; for the question of its constitutionality, see Arzt, NVwZ 2013, 1328 – 1332; for more, see also *Töpfer*, Informationsaustausch, passim.

[428] For the general structure of the intelligence services, see also *Engelhart*, The Secret Service's Influence, at 506 ff.; *Rose-Stahl*, Recht der Nachrichtendienste, 15.

vices consist of the Federal Intelligence Service (*Bundesnachrichtendienst:* BND),[429] the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz:* BfV)[430], and the Military Counterintelligence Service (*Bundesamt für den Militärischen Abschirmdienst:* MAD).[431] We will restrict ourselves to the services of the federation, primarily the BND and the BfV, as they are the main suppliers of intelligence information for criminal investigations. In the field of domestic security, the *Länder* set up 16 State Offices or Departments for the Protection of the Constitution (*Länderverfassungsschutzämter* or *-abteilungen*). As for the intelligence services at the *Länder* level, there are some far-reaching transfer powers in force, but there is no unified concept for the transfer of intelligence information.[432] If intelligence information is transferred from the domestic intelligence service of one *Land* to the criminal prosecution authorities of another *Land*, the federal provisions apply.[433] However, the federal provisions do not apply if information is transferred from a domestic intelligence service to the criminal prosecution authorities of the same *Land*.[434] This is why it is argued that the abovementioned informational separation between the intelligence services and the police applies only at the federal level but not between the security authorities of one *Land*.[435] Yet, the German Federal Constitutional Court does not distinguish between the intelligence services at the federal and at the *Länder* level when it emphasizes that information sharing between the intelligence services and the police authorities is principally not permitted.[436]

### *b) Unsolicited information transfer*

Intelligence services are obligated to communicate their information, including personal data,[437] to the responsible public prosecutor's office and to the police if

---

[429] *Engelhart*, The Secret Service's Influence, at 511; *Sieber*, NJW 2008, 882; *Arslan*, Intelligence and Crime Control, 514; *Zöller*, JZ 15/16/2007, 765.

[430] *Arslan*, Intelligence and Crime Control, 515; *Zöller*, JZ 15/16/2007, 765; *Engelhart*, The Secret Service's Influence, 510.

[431] For more, see *Engelhart*, The Secret Service's Influence, 511; *Daun*, Die deutschen Nachrichtendienste, 59 and 63.

[432] *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 480; see also *Greßmann*, Nachrichtendienste und Strafverfolgung, 407.

[433] § 21 para 1 BVerfSch-Gesetz.

[434] Ibid.

[435] *Singer*, Die Kriminalpolizei 2006, 114; compare *Graulich*, Sicherheitsrecht des Bundes, 9, who argues that the principle of separation does not apply to the organization of the security agencies at the Länder level, whereas these agencies must in fact adhere to the same principle in the event of an information transfer.

[436] BVerfG NJW 2013, 1505.

[437] For a definition of 'information' and 'personal data', see *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 298 ff.

there are factual indications that such sharing is necessary to (prevent or) prosecute a crime against national security.[438] The required threshold is similar but lower than the so-called initial suspicion in criminal proceedings. Still, mere assumptions are not sufficient grounds for a transfer.[439] The information in question must enable the criminal prosecution authorities to seriously consider the possibility of criminal investigations against the person concerned for an offence against national security.[440] However, the intelligence service will assume the presence of suspicion related to enumerated offences against national security.[441] In addition to offences against national security, the intelligence law stipulates the transfer of information if the crime in question is politically motivated. This requirement is met if there are factual indications that, based on the offender's objectives and motivation or his or her connection with an organization, the offence that was committed was directed against the free democratic basic order, the existence and security of the Federal State and the *Länder*, or against Germany's external interests.[442] Thus, the scope of unsolicited transfer is de facto expanded to almost all types of crime, including petty theft, provided there is a link to the protection of the aforementioned values.[443]

The intelligence services are obligated to transmit, unsolicited, available intelligence information on crimes against the security of the state to the public prosecutor's office and to the police but not to the criminal courts. However, after the public prosecutor has filed the indictment, he or she is required to forward any intelligence information received from the services to the trial court.[444]

Besides the information transfer related to national security offences, including politically motivated crimes in a broad sense, intelligence services are also author-

---

[438] § 20 para 1 BVerfSch-Gesetz; for these crimes see *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 318 ff.; *Nehm*, NJW 2004, 3294; for the necessity of information sharing with the criminal prosecution authorities in the area of what is called state protection, see *Greßmann*, Nachrichtendienste und Strafverfolgung, 402 and 407; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 291 complains about the lack of jurisprudence on the unsolicited transfer of information in case of crimes against national security; see also *Engelhart*, The Secret Service's Influence, 520.

[439] *Lang*, Geheimdienstinformationen, 94 f.; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 308 ff.

[440] Ibid.

[441] In §§ 74a and 120 GVG.

[442] § 20 para 1 BVerfSch-Gesetz; *Greßmann*, Nachrichtendienste und Strafverfolgung, 408.

[443] *Lang*, Geheimdienstinformationen, 95; considering, inter alia, the unspecified catalogue of crimes against national security in a broad sense, *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 357, concludes that § 20 para 1 BVerfSch-Gesetz is unconstitutional.

[444] For more see *Engelhart*, The Secret Service's Influence, 527; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 348 ff.

ized to forward information including personal data to the police and the public prosecutor's office if the communication in question is 'necessary to prevent or otherwise avert or prosecute crimes of significant importance'.[445] The exercise of the third statutory power is at the discretion of the intelligence services as the law reads 'may … submit'.[446] However, the law stipulates an important exception and restricts the discretion of the federal domestic intelligence service (BfV) if there are sufficient indications to suggest that a covert agent of the service itself unlawfully committed an offence of 'significant importance'. In this case, the public prosecutor's office must be immediately informed about the suspicion. But the president of the agency is allowed to depart from this obligation.[447] As a result, the discretion of the services is not reduced to 'zero' in such cases.[448]

In fact, at least under the third statutory power, the intelligence services gained considerable influence in the criminal prosecution of certain serious crimes as they are now not only in the position to provide the criminal prosecution authorities with information on a broad spectrum of offences, but they can also decide whether or not to trigger criminal prosecution.[449] It is worth noting that, in terms of the discretionary power of the intelligence services, the law provides no threshold, namely, whether the information at issue gives rise to a certain type of suspicion.

Furthermore, the law has separate provisions for the unsolicited transfer of intelligence information the services collected by means of telecommunication interception, residential surveillance, and the so-called IMSI-catcher, as they constitute a serious interference with the basic rights of the persons concerned.[450] Information so gathered for intelligence purposes may be transferred to the police authorities for purposes of prevention or prosecution if there are factual indications to suspect that someone is planning, committing, or has committed an enumerated crime.[451] De-

---

[445] § 19 para 1 nos 3 and 4 BVerfSch-Gesetz.

[446] For further details, see *Greßmann*, Nachrichtendienste und Strafverfolgung, 408; see also *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 353.

[447] § 9a para 2 BVerfSch-Gesetz.

[448] See also *Greßmann*, Nachrichtendienste und Strafverfolgung, 409; for the scope of the duty of intelligence services to report crimes, see *Engelhart*, The Secret Service's Influence, 525.

[449] Compare *Engelhart*, The Secret Service's Influence, 514, who points out that particularly the BND 'can be seen as secret criminal police agency'; see also *Arslan*, Intelligence and Crime Control, 527 ff.; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 337 and 439 ff.; *Lang*, Geheimdienstinformationen, 101; Gleß, Predictive policing, 175.

[450] §§ 4 para 4 nos 2, 7 para 4., 8 para 6 G10-Gesetz; §§ 9 paras 2 and 4 BVerfSch-Gesetz; for more see *Greßmann*, Nachrichtendienste und Strafverfolgung, 407; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 484; *Engelhart*, The Secret Service's Influence, 520; for the surveillance of telecommunication by the services see *Huber*, NJW 2013, 2572 ff.

[451] §§ 4 para 4 nos 2, 7 para 4., 8 para 6 G10-Gesetz; see also *Engelhart*, The Secret Service's Influence, at 520; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 426 ff.

spite the complicated reference technique the G10 Act uses for the enumeration it is evident that the crimes in question involve not only acts against national security, acts of international terrorism, and serious crimes against the individual such as homicide, but also organized theft and other serious variations of robbery, fraud, or money laundering. As a result, the unsolicited transfer in accordance with the G10 Act is ultimately based on the principle that intelligence gathered using the means described may also be transferred if the information involves 'crimes of significant importance', even though the G10 Act requires meeting a certain threshold of suspicion, unlike the corresponding provision in general intelligence law. An unsolicited transfer of intelligence in keeping with the G10 Act is also at the discretion of the intelligence services.[452]

Finally, the issue of whether or to what extent the intelligence services have the obligation or the power to transfer information to the criminal prosecution authorities in parallel to the above-mentioned provisions based on so-called 'administrative assistance' is controversial.[453] This question arose in 2008 in the context of the Liechtenstein scandal, where the German foreign intelligence service (BND) assisted a local tax investigation department in buying stolen bank account information from a former employee of a foreign bank for purposes of investigating tax evasion.[454] Although a general obligation of the BND to support domestic authorities in investigations abroad is accepted,[455] it is not considered to be within the competence of the BND to actively collect information on tax evasion and to communicate it to the tax investigation authorities of its own accord and on its own responsibility.[456] Otherwise the above-mentioned limits on information transfer would become obsolete.[457] The use of illegally obtained intelligence information in criminal proceedings will be explored below.[458]

### *c) Transfer on request*

The police or the criminal prosecution authorities may also ask the intelligence services for a transfer of information the requested agency already has at its disposal

---

[452] *Engelhart*, The Secret Service's Influence, 525; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 425.

[453] For more see *Engelhart*, The Secret Service's Influence, 519 f.; compare *Soiné*, Aufklärung der Organisierten Kriminalität, 13.

[454] See fore more *Sieber*, NJW 2008, 881; *Engelhart*, The Secret Service's Influence, 525 f.

[455] *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 557.

[456] *Sieber*, NJW 2008, 886; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 558; *Engelhart*, The Secret Service's Influence, 526.

[457] *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 558 f.

[458] See below IV.C.4.a) Illegally collected evidence.

or which they can infer from open sources.[459] By restricting the request to information already acquired or publicly available, the law's objective is to avoid situations where the police or the criminal prosecution authorities request the intelligence services to conduct investigative measures and search for (new) information on their behalf. In fact, this is one of the consequences of the constitutionally mandated principle of separation.[460]

If a request by the police or the criminal prosecution authorities involves the transfer of personal data, German law requires what is called a double authorization: not only the authority in possession of the information must be allowed to transmit but the authority requesting the transfer must also be permitted to request, as both actions (transfer and corresponding request) constitute, each by itself, an interference with the constitutionally guaranteed right to informational self-determination.[461] As mentioned above, § 161 para 1 CCP entitles 'the public prosecution office … to request information from all authorities', including the intelligence services.[462] However, this does not mean that the services are obligated or allowed to transfer all requested information to the criminal prosecution authorities pursuant to the above provision of the CCP.[463] As said, the latter merely enables the public prosecutor's office to ask for intelligence information. The transfer itself is still subject to the above-mentioned requirements under intelligence law.[464] At this point it is important to mention that the trial court can also seek information from the intelligence services.[465]

### 3. Suspending a Transfer

A transfer of intelligence information to the police, the public prosecutor's office, or the courts, whether unsolicited or on request, must not be executed in the following cases:

---

459 § 17 para 1 BVerfSch-Gesetz.

460 Compare § 8 para 3 BVerfSch-Gesetz; for the scope and limits of the principle of separation in German law, see *Engelhart*, The Secret Service's Influence, 509; *Arslan*, Intelligence and Crime Control, 510 f.; *Lang*, Geheimdienstinformationen, 105; *Gusy*, KritV 1994, 242–251; against a broad interpretation of the principle of separation *Nehm*, NJW 2004, 3290 f.

461 BVerfGE 65, 1 ff.; *Greßmann*, Nachrichtendienste und Strafverfolgung, 406.

462 *Engelhart*, The Secret Service's Influence, 524.

463 *Greßmann*, Nachrichtendienste und Strafverfolgung, 409; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 504 f.

464 In particular to §§ 19 para 2 nos 1–4, 20 para 1 BVerfSch-Gesetz and 4 para 4 no 2, 7 para 4, 8 para 6 G10-Gesetz; see also *Engelhart*, The Secret Service's Influence, 520.

465 § 202, 244 para 2 StPO; see also *Engelhart*, The Secret Service's Influence, 527; *Greßmann*, Nachrichtendienste und Strafverfolgung, 410.

– if the legitimate interests of the person concerned outweigh the public interests in communicating the information in question (i.), or
– if other public interests, notably security interests, require the withholding of the information in question (ii.), and
– if a specific law prohibits a transfer (iii.).[466]

Decisions to suspend an information transfer despite its relevance for criminal prosecution purposes are made by the services themselves. The law does not stipulate a prior judicial review.[467] A 'non-disclosure' decision at this stage of criminal proceedings may restrict not only the obligation and power of the criminal prosecution authorities to 'make investigations of any kind'[468] and to 'ascertain not only incriminating but also exonerating circumstances'[469] but also, particularly in the latter case, the rights of defence. If it is informed in the first place, all the defence can do is to challenge the legality of the non-disclosure decision by the services before the administrative court; however, the practicability of this remedy remains in doubt.[470]

The protection of personal interests will lead to the suspension of a transfer of information if the personal data relate to the so-called core area of privacy. Such data must not be transmitted.[471] The transfer of information is also restricted in case of minors.[472]

The second reason for withholding intelligence information from the public prosecutor's office or the police, namely security interests, is particularly relevant.[473] Security interests are, *inter alia*, the interests of the services in using their 'sources' in pending or future investigations and in protecting their methods and techniques.[474] In this regard, the notion of security interests, which may lead to suspend a transfer of intelligence information by the services to the public prosecutor or the police, is quite similar to the notion of state secrets within the meaning of §§ 54 and 96 CCP (more explanations on that below),[475] although the protection

---

466 § 23 para 1 BVerfSch-Gesetz; for more see *Lang*, Geheimdienstinformationen, 95; *Greßmann*, Nachrichtendienste und Strafverfolgung, 410.

467 *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 363.

468 § 160 para 1 StPO.

469 § 160 para 2 StPO; for more see *Kröpil*, JuS 2015, 241.

470 *Engelhart*, The Secret Service's Influence, at 527; see also *Marsch*, Germany, 108.

471 BVerfG NJW 2016, 1786; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 361.

472 § 24 BVerfSch-Gesetz.

473 *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 362.

474 *Greßmann*, Nachrichtendienste und Strafverfolgung, 410; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 364 f.; *Engelhart*, The Secret Service's Influence, 520; see also *Frisch*, Schutz staatlicher Geheimnisse, 205; *Kudlich*, JuS 2004, 929.

475 See below IV.C.2.a) General framework.

of state secrets is grounds for rejecting a trial court's request for disclosure of evidence.[476] However, the different nature of relations between the intelligence services and the public prosecutor's office or police and the trial courts should not be overlooked.[477]

In fact, a closer look reveals that when the services share information with the public prosecutor's office or the police they employ practices that exist in parallel with the suspension provisions of intelligence law and the aforementioned provisions of the CCP. The most prominent practice is to communicate relevant information in return for a promise by the public prosecutor's office or the police that the information will not be added to the official case file. In practice, such information is labelled 'not for use by the court' (*nicht gerichtsverwertbar*). In this way, the services save themselves from having to make a formal decision on grounds of the aforementioned provisions, and they also meet their objective of keeping their sources protected by trusting the integrity of the public prosecutor's office or the police.[478] Aside from questions whether this practice is covered by intelligence law[479] and, for the public prosecutor's office, by criminal procedure law, the impact on the defendant's defence rights is considerable. As a result of the promise, the defence (and the trial court) will not be routinely notified about the existence of relevant intelligence information, and the decision not to disclose the information will routinely be taken unilaterally.[480] This practice of non-disclosure by the services and the criminal prosecution authorities not only creates 'undisclosed incriminating evidence'[481] in criminal proceedings but also risks violating the right to a fair trial as interpreted by the European Human Rights Court.[482]

---

476 *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 366.

477 See also *Engelhart*, The Secret Service's Influence, 519.

478 For more, see *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 384 ff.

479 At least for intelligence information transmitted on grounds of § 19 para 1 BVerfSch-Gesetz, one can argue that the receiver of the information, namely the public prosecutor's offices and the police, are obligated to comply with the purpose of the transmission in accordance with § 19 para 1 BVerfSch-Gesetz. This provision expressly stipulates the receiver's obligation to use the transmitted intelligence information only for the purpose underlying the transmission itself. Thus, the provision entitles the intelligence services to define the purpose to which the public prosecutor's offices or the police may use the information received.

480 *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 389 f.; compare the requirements the public prosecutor must meet in order to withhold the so-called 'files of indicators' (Spurenakte) resulting from investigations against third persons, see BVerfG NJW 1983, 1043–1046; BVerfG NStZ-RR 2013, 379–380 (search warrant based on undisclosed evidence).

481 Compare *Marsch*, Germany, 107.

482 ECtHR, Judgment of 16 Feb. 2000 – 28901/95 (Rowe and Davis v. The United Kingdom), § 65 ('the prosecution's failure to lay the evidence in question before the trial judge and to permit him to rule on the question of disclosure deprived the applicants of a

### 4. Use of Intelligence Information

Having explained the relevant provisions of criminal procedure law with regard to requests for intelligence information for evidentiary purposes and the respective provisions of intelligence law regarding the information transfer, the use of intelligence information for criminal investigation purposes should be explored as well. In fact, the last-named concern seems redundant because any restriction on the use of transferred information goes against the common perception that there is no doubt that the criminal prosecution authorities will use any intelligence information, once it is transmitted and received. However, as mentioned above, the use of intelligence information by the criminal prosecution authorities requires further legal basis, because this also constitutes an interference with the constitutionally protected right to informational self-determination.[483]

The framework for using personal data collected according to a different law than the Code of Criminal Procedure is provided in § 160 paras 2 and 3 CCP, which are regulations for use by the public prosecutor and the trial court.[484] If the court is not permitted to use a specific type of information, this amounts to a restriction of the court's duty to conduct *ex officio* searches for the truth (§ 244 para 2 CCP).[485] The restriction includes intelligence information gathered not only in pursuit and for purposes of intelligence law but in most cases also without any suspicion of crime.[486] Thus, allowing the use of intelligence information collected for different purposes and employing lower thresholds in applying intelligence techniques in criminal proceedings create the risk of obsolescence not only of the constitutionally mandated protection of personal data but also of the guarantees for individuals in the CCP. In particular, the CCP limits the powers of the criminal prosecution authorities to interfere with the basic rights and freedoms, *inter alia* by subjecting the application of secret investigation measures to some degree of suspicion and to investigations of serious crimes.[487] The question arises how to maintain this level of protection under the CCP in cases where the intelligence services have already collected personal information relevant to the criminal prosecution. In other words, what can the legislature do to prevent that the intelligence services bypass the constitutional guarantees by dominating criminal proceedings or by escaping

---

fair trial'); ECtHR, Judgment of 24 June 2003 – 39482/98 (Dowsett v. The United Kingdom), § 44.

483 See above IV.B.2.a) General framework.

484 *Lang*, Geheimdienstinformationen, 114.

485 For more, see below IV.C.1. a) Principles of evidence taking by the court.

486 *Engelhart*, The Secret Service's Influence, 513; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 521.

487 On the main features of the intelligence investigations and distinctions between intelligence and repressive police investigations, see *Arslan*, Intelligence and Crime Control, 515.

from the CCP to intelligence law? To this effect, § 160 para 2 CCP restricts the use of information not gathered under the Code but under a different law, *inter alia*, intelligence law, to two cases:

– first, if the person concerned consents to the use of intelligence information
– second, if the measure that led to the collection of the intelligence information at issue could hypothetically also have been ordered under the CCP (the so-called hypothetical order).

The first alternative will predominantly apply if the information exonerates the defendant and the latter consents as expected. In the second case, the use of intelligence information must be justified by applying the so-called hypothetical order. Although details still need to be clarified and are controversial,[488] this order mandates that the requirements of the CCP be met as far as possible and in analogy with it at the very time when the criminal prosecution authorities make use of the intelligence information in question. The important factors for an analogous application of the CCP to the intelligence gathering process in question are, in particular, the type of measures applied, the threshold of suspicion, and the type of crime at stake.

The first condition is that the measure used by the intelligence services to collect the information at issue is also allowed under the CCP, i.e. dragnet investigation, interception of telecommunication, use of technical means, photography, other surveillance devices, IMSI-Catcher, and undercover investigators.[489] In this way, the law prohibits the use of intelligence information collected by measures which only the services can use and which are unavailable to the criminal prosecution authorities.[490] This enables the legislature to prevent situations where certain highly intrusive secret measures employed by the services also have implications for criminal proceedings (this would challenge the proportionality of these measures) but also the notion that the criminal prosecution authorities can count on the privileges of the intelligence services. For instance, investigation measures such as the so-called visual residential surveillance or strategic surveillance are not available to the criminal prosecution authorities in Germany as the CCP lacks corresponding provisions. Under § 160 para 2 CCP, intelligence information gathered by these measures must not be used in criminal proceedings, at least not directly.[491]

Moreover, the analogous application of other criteria, namely the threshold of suspicion and the type of crime in question, can only be undertaken retrospectively and thus hypothetically, because neither did the collection of intelligence infor-

---

488 For more, see *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 524 ff.

489 §§ 98a, 100b, 100f, 100h, 100i, and 110a StPO; for more, see *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 534 f.

490 *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 522.

491 *Lang*, Geheimdienstinformationen, 127 f.

mation occur for purposes of a criminal investigation nor did the services, at the time, act on the assumption of a certain suspicion of a crime within the meaning of the CCP. As a result, a subsequent use of said information requires a hypothetical assumption about whether the measure in question could have been ordered under the CCP at the time the information was subsequently used. Therefore, a certain degree of suspicion must have been reached so that the measure could, even if hypothetically, have been ordered at the time of the use of intelligence information in question. However, this does not mean that the suspicion must exist independent of the intelligence information transferred. Provided this information was transmitted voluntarily and according to intelligence law, it may also form the basis for the suspicion.[492] Due to the fact that unsolicited transmitted intelligence information can substantiate a certain degree of suspicion in most cases, the proof whether its use is allowed pursuant to §160 para 2 CCP will largely depend on the existence of a relevant crime and a relevant measure as mentioned above.

The information may only be used for the prosecution and adjudication of the crime that is subject to both the transfer regulations and the evidence rule of § 160 para 2 CCP.[493]

However, it must be noted that §160 para 2 CCP governs and restricts only the direct use of intelligence information in criminal proceedings. The indirect use in the form of tips or leads by the criminal investigation authorities to collect further evidence or to locate a suspect's whereabouts is allowed without recourse to this provision.[494] As long as the criminal prosecution authorities limit themselves to this indirect use of intelligence information, they will also produce 'undisclosed incriminating evidence' at the investigation stage because, in most cases, the defendant will not be informed of the use or the existence of the information. The European Court of Human Rights seems to consider this practice compatible with the right to a fair trial, provided the defendant subsequently has the possibility to challenge the legality of the measures conducted against him or her.[495] However, this practice means in terms of national law that intelligence information gathered by secret investigative measures not allowed under the CCP, such as strategic surveillance, can also be introduced to criminal investigations.[496] Furthermore, § 160 para 2 CCP

---

[492] For more, see *Lang*, Geheimdienstinformationen, 113.

[493] See § 19 para 1 BVerfSch-Gesetz; *Lang*, Geheimdienstinformationen, 115.

[494] *Greßmann*, Nachrichtendienste und Strafverfolgung, 416; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 532; *Lang*, Geheimdienstinformationen, 115; *Arslan*, Intelligence and Crime Control, 523; critical, *Hefendehl*, GA 2011, 225.

[495] ECtHR, Judgment of 20 Nov. 1989 – 11454/85 (Kostovski v. The Netherlands), § 44; on the use of intelligence information to arrest suspects, see ECtHR, Judgment of 28 Oct. 1994 – 14310/88 (Murray v. The United Kingdom), § 58 (the use of confidential information is essential in combating terrorist violence and the threat that organized terrorism poses to the lives of citizens and to democratic society as a whole).

[496] But see *Gercke*, CR 11/2013, 752.

governs only the use of personal data collected by certain intrusive secret investigative measures. Intelligence information that does not consist of personal data or is collected by less intrusive investigation measures can be used based on 160 para 1 CCP.[497]

## 5. Interim Results

The transfer and use of intelligence information in criminal proceedings in Germany are subject to extensive regulations. This is a result of the jurisprudence of the German Constitutional Court on the right to informational self-determination in the early 1980s. Not just the intelligence service that transfers the information requires specific provisions justifying the transfer of personal data to the criminal prosecution authorities, but the latter, as the requesting or receiving authority, must have corresponding powers as well. The informational separation between the intelligence services and the police authorities allows, at least according to the Court, departures from the main principle only by exception. The intelligence services are allowed to render a 'non-disclosure' decision, inter alia for reasons of security interests or for the protection of state secrets. The defendant can challenge this decision before the administrative court, provided he or she was informed. Moreover, in order to use the intelligence information received, the public prosecutor's office must pass a certain test. If it is passed, the public prosecutor's office may restrict access to the investigation files for the defence, and the use and existence of intelligence information may remain unknown to the defence ('indirect evidence' at investigation stage).[498] However, the public prosecutor's office must disclose all evidence in support of the indictment, at the latest after charges against the defendant have been filed in trial court. If the public prosecutor seeks further protection for the intelligence information or other evidence related to state secrets, he or she may apply measures provided in the CCP, which will be explored below ('indirect evidence' at trial stage).

These are the basic structural outlines of the information transfer and the criminal procedure law regarding the transfer, receipt, and use of intelligence information in criminal proceedings. However, the fact that questions are waiting to be clarified and that long-standing and established practices exist for the transfer and use of intelligence information should not be overlooked. The scope of administrative cooperation between the intelligence services and the criminal prosecution authorities, the construction of 'not for use in court as evidence', and the indirect use of intelligence as investigative tips (both 'undisclosed incriminating evidence' at the investigation stage) are implicated in blurring the boundaries of the basic

---

497 *Lang*, Geheimdienstinformationen, 116.

498 *Engelhart*, The Secret Service's Influence, 528.

structure, thereby creating a space where the authorities can enjoy a high degree of flexibility. At the same time it must be noted that the non-disclosure of intelligence information by the criminal prosecution authorities in particular violates the defendant's right to a fair trial.

In the final analysis, the strict separation of intelligence from criminal prosecution based on the constitutionally mandated principle of separation appears not to exist, at least in some areas of crime. In practice, the power of this principle is not imperative, at least with regard to separation in terms of information, in obvious contrast to the above-mentioned jurisprudence of the Constitutional Court.[499] Only the organizational separation continues to carry much weight.[500]

## C. Use of intelligence information and protection of state secrets at the trial stage

### 1. Trial procedures and main principles

#### a) Principles of *evidence* taking by the court

##### aa) Constitutional framework

The objective of criminal proceedings is to facilitate the application of the state's monopoly on punishment by the judiciary for the sake of protecting the legal interests of the public and of individuals.[501] In other words, criminal proceedings must meet the objectives of substantive criminal law, in particular to protect society's most valuable legal interests and to punish perpetrators who significantly harm or endanger them in a blameworthy manner (culpability principle).[502]

Most importantly, the requirements of substantive criminal law compel criminal courts to search ex officio for the material truth.[503] This means that the court hearing must be conducted in order to establish the so-called material truth about the defendant's guilt and the facts relevant to sentencing (the so-called principle of ex officio inquiry). Accordingly, § 244 para 2 CCP requires the court to search for the

---

499 *Arzt*, NVwZ 2013, 1332.

500 *Engelhart*, The Secret Service's Influence, 509 and 515; see also BVerfG NJW 2013, 1502.

501 BVerfG NJW 2010, 593.

502 BVerfG NJW 2016, 1153; BGH NStZ 2015, 170; *Vogel*, The Core Legal Concepts and Principles, 54.

503 BVerfG NJW 1983, 1043; for a critical perspective on the notion of material truth, see *Schünemann*, Reflexionen über die Zukunft des deutschen Strafverfahrens, 474 ff.; on a comparison between the notions of material truth and consensual truth as mutual alternatives, see *Weßlau*, ZIS 1/2014, 561 ff.; on the notion of the so-called procedural truth, see *Link*, Wahrheit und Gerechtigkeit, 103 f.

truth and, consequently, to 'proprio motu, extend the taking of evidence to all facts and means of proof relevant to the decision'.[504] The determination of material truth will enable the trial court to apply the standards of criminal liability and sentencing. In other words, if there is no material truth, the trial court cannot establish guilt or innocence or issue the corresponding sentence.[505] According to this concept of criminal proceedings, the public prosecutor and the defendant have no authority to decide on the findings of fact and the legal merits of the case.[506] However, the CCP recognizes some exceptions to the court's duty and power to take and use all relevant evidence. In particular, there are other public institutions also vested with the power to withhold from the court, in part or in whole, information or documents qualified as state secrets. This is not only true for the above-explored provisions of intelligence law on the suspension of a transfer of intelligence information to the criminal prosecution authorities including the trial court; rather, §§ 54 and 96 CCP also explicitly stipulate limits on the court's possibilities to obtain evidence (more on that below).[507] Moreover, German criminal procedure law recognizes several exclusionary rules of evidence that preclude obtaining or admitting certain types of evidence. These rules apply inter alia where intelligence information was collected illegally, such as by torture abroad,[508] or where personal data about the so-called core area of privacy are involved. Such information must be excluded from criminal proceedings.[509]

In terms of the constitutional requirements for criminal proceedings in Germany, Art. 92 Basic Law specifically stipulates that only a judge can impose criminal sanctions.[510] Only very few guidelines can be inferred from this constitutional requirement with regard to the question of how a criminal court should proceed in order to comply with the principles of culpability and material truth. At a minimum, the judge must independently establish all factual circumstances necessary for his or her judgment on guilt or innocence and for sentencing. The factual and legal assessments of other institutions, particularly of the investigation authorities, must not be adopted without further inquiry. A blind adoption of evidence collected by the prosecution authorities into a judge's decision-making process is prohibited

---

504 Emphasis added; translation by Brian Duffett and Monika Ebinger, available at https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p1647; for more, see BVerfG NJW 1981, 1719–1726, 1723; BVerfG NJW 2003, 2444–2447, 2445; Fezer, StV 1995, 263.

505 BVerfG NJW 1981, 1722; BVerfG NJW 2013, 1060, 1067; BVerfG NStZ 2016, 424; BVerfG NJW 2016, 1153; *Weigend*, GLJ 15/2014, 84 f.; *Weßlau*, ZIS 1/2014, 558.

506 See § 264 para 2 StPO; BVerfG NJW 1981, 1723; BVerfG NJW 2013, 1062; BVerfG NStZ 2016, 424.

507 BVerfG NJW 1981, 1723; see below IV.C.2.a) General framework.

508 For more, see below VI.C.4.a) Illegally collected evidence.

509 BVerfG NJW 2016, 1787; *Lang*, Geheimdienstinformationen, 117 f.

510 See also BVerfG NJW 1967, 1219, 1221; *Bürger*, ZStW 128(2)/2016, 518.

under the constitution.[511] The same applies mutatis mutandis to the evaluation of information by the intelligence services and to their decisions on the conditions for withholding or introducing information.[512]

bb) Statutory framework

The CCP has provisions that compel the judge to adhere to the principle of immediacy in taking evidence and reaching a judgment. The Code formally requires the judge to conduct an independent and comprehensive inquiry into the facts and to base his or her judgment on the evidentiary results of his or her own hearing.[513] The principle of formal immediacy is supposed to enhance the separation of the evidentiary results of the investigation and those at the trial stage and emphasizes the value of personal evidence-taking by the judge in order to make a decision.[514] This is not only in the public interest as the public nature of the main hearing allows the public to understand the validity of a criminal judgment, but it serves to control the judiciary and to protect the defendant from misuse of power.[515] In its substantive function the principle of immediacy requires the judge who is seeking to prove both facts in favour and against the indictment to select the evidence closest to the facts.[516] This is best illustrated in § 250 para 1 CCP, which stipulates the primacy of the examination of a person by the judge over the introduction of documents relating to his or her previous statements.[517] The rationale behind this is that in the court's search for material truth an examination of witnesses or experts in person is deemed to produce a more qualified assessment of their reliability and credibility.[518] However, the CCP permits, to the detriment of the defendant, important exceptions to this primacy of orality and immediacy, based not only on the mutual consensus of the judge, the public prosecutor, and the defence[519] but also in the interest of the public and other individual interests (e.g. inter alia for the protec-

---

[511] *Bürger*, ZStW 128(2)/2016, 519 f.; *Dumitrescu*, 130(1)/2018 ZStW, 107; see also BGH NJW 1998, 1164; BGH NStZ 2015, 170.

[512] See also below IV.C.2.b)cc) Written statements and hearsay witnesses.

[513] See §§ 244 paras 2 and 261 StPO; *Dumitrescu*, 130(1)/2018 ZStW, 110; *Theile*, ZIS 1/2013, 128; *Jahn*, StV 2015, 779; compare, however, *Pollähne*, StV 2015, 788.

[514] BGH Decision 22 May 2013 – 4 StR 106/13, BeckRS 2013, 10079; for more see *Pollähne*, StV 2015, 787.

[515] *Bürger*, ZStW 128(2)/2016, 525.

[516] *Bürger*, ZStW 128(2)/2016, 520; *Dumitrescu*, 130(1)/2018 ZStW, 107 f.; *Theile*, ZIS 1/2013, 128; *Pollähne*, StV 2015, 788; *Jahn*, StV 2015, 779.

[517] BVerfG NJW 1981, 1722; *Vogel*, The Core Legal Concepts and Principles, 65; *Engelhart*, The Secret Service's Influence, 530; *Dumitrescu*, 130(1)/2018 ZStW, 111.

[518] *Bürger*, ZStW 128(2)/2016, 525; see also BVerfG NJW 1981, 1722.

[519] § 251 para 2 StPO; see also *Theile*, ZIS 1/2013, 131.

tion of state secrets).[520] Thus, it allows the use of so-called hearsay evidence introduced by surrogates, i.e. the reading of previous statements, other official reports, or the hearing of secondary witnesses who interrogated the original witnesses.[521] Allowing the use of 'indirect evidence' in a criminal trial is very important for the public authorities, particularly for the intelligence services and police authorities, both to protect their secrets and to introduce evidence into trial (more on that below).[522] The legal problem that arises in evidence taking is that the German criminal procedure system is based on the principle of examination in person (§ 250 para 1 CCP). To that extent there is a conflict between the law of evidence and the interests in secrecy.[523] The German Constitutional Court recognizes that the use of hearsay evidence in accordance with § 250 f CCP does not violate the constitutional principles of procedure or the defence rights, in particular the right to be heard.[524] The defendant's constitutionally guaranteed right to be heard by the court in accordance with the law[525] does not establish a right to immediacy of evidence taking or the prohibition of hearsay evidence.[526]

Furthermore, the CCP typically requires that the court's decision on guilt or innocence and the sentence must be based on evidence taken in line with the principles of immediacy and orality.[527] Whereas the court is compelled to follow strict principles of evidence-taking during the main hearing,[528] it is not bound by certain rules of evidence in arriving at its decision (principle of freely formed conviction).[529] In case of intelligence information or other evidence which the court could only consider subject to limitations on the principles of material truth, immediacy, or on the defence rights, the courts should routinely consider such circumstances as diminishing the value of the evidence in question.[530] In addition, it is generally

---

[520] See below IV.C.2.a) General framework.

[521] See §§ 251 ff. StPO; BVerfG NJW 1981, 1719–1726, 1721; *Dumitrescu*, 130(1)/2018 ZStW, 113 ff.; *Vogel*, The Core Legal Concepts and Principles, 65.

[522] See below IV.C.2.a) General framework.

[523] Für more on this, see *Frisch*, Schutz staatlicher Geheimnisse, 205.

[524] BVerfG NJW 1981, 1722; BVerfG NStZ-RR 2013, 115; BVerfG NJW 1996, 449; BVerfG NJW 1992, 168.

[525] Art. 103 para 1 Basic Law.

[526] BVerfG NJW 1953 177–178, 178; see also *Marsch*, Germany, 108 f.; *Kudlich*, JuS 2004, 930.

[527] For more, see §§ 260, 264 StPO; see also BGH Judgment, 20 Dec. 1977, Case no: 5 StR 676/77; OLG Hamm NJW 1973, 1427 ff.; see also *Dumitrescu*, 130(1)/2018 ZStW, 112; *Jahn*, JuS 2007, 193; *Pollähne*, StV 2015, 789; *Klesczewski*, HRRS 1/2004, 14.

[528] *Alsberg*/*Dallmeyer*, Der Beweisantrag im Strafprozess, at 237; *Klesczewski*, HRRS 1/2004, 14.

[529] On the scope and limits of the principle of freely formed conviction in criminal proceedings, see BVerfG NJW 2003, 2445 f.; see also *Fezer*, StV 1995, 95–101; *Vogel*, The Core Legal Concepts and Principles, 64.

[530] See below IV.C.2.b)cc) Written statements and hearsay witnesses.

accepted that the court should pay due attention to the fact that intelligence information is mostly one-sided or may even present events in a distorted manner. These factors will therefore regularly lead the trial court to assume a lower evidentiary value for intelligence information.[531] A similar problem, i.e. the diminished value of intelligence information as evidence in criminal proceedings, arises if the information consists only of analyses carried out by the services and lacks the 'raw facts' underlying these analyses. Such situations require the due attention of the court in applying the strict criteria of evidence evaluation in keeping with § 261 CCP.[532]

### *b) Rights of defence*

#### aa) Constitutional framework

The constitution provides the foundation and many guarantees for the rights of the defence in criminal proceedings.[533] Especially the provisions on freedom of the person (Art. 2 para 2 Basic Law) and on human dignity (Art. 1 para 1 Basic Law) provide certain minimum standards for an effective participation by the defendant in criminal proceedings, considering that the outcome of the proceedings might considerably restrict the defendant's personal freedom and that a potential moral condemnation associated with a conviction would also impair his or her dignity.[534]

The respect for the defendant's dignity requires that he or she not be degraded to a mere object of criminal proceedings.[535] In addition, the rule of law requires a fair trial[536] for the defendant, and the constitution explicitly enshrines the defendant's right to be heard (Art. 103 para 1 Basic Law).[537]

More specifically, in conjunction with the respect for the defendant's dignity, the constitutionally guaranteed right to be heard requires to 'give him the opportunity to safeguard his interests and to have influence on the course and the outcome of the proceedings'. In other words, the defendant must be given the 'opportunity to

---

[531] *Lang*, Geheimdienstinformationen, 119; see also *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 298; for more see below IV.C.2.b)cc) Written statements and hearsay witnesses.

[532] BGH Decision 26 March 2009, Case no: StB 20/08, HRRS 2009 no 550, at 31; *Lang*, Geheimdienstinformationen, 119; see also *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse, 304; on the constitutional limits of § 261 CCP, see BVerfG NJW 1981, 1722.

[533] See generally BVerfG NJW 2007, 205.

[534] BVerfG NJW 1981, 1722; see also BVerfG NJW 2003, 2445; BVerfG NStZ-RR 2013, 115.

[535] BVerfG NJW 1981, 1722; see also BVerfG NStZ-RR 2013, 115.

[536] BVerfG NJW 2013, 1060; BVerfG NJW 1981, 1722.

[537] For more, see BVerfG NJW 1981, 1721; BVerfG NJW 1983, 1043.

comment on the facts relevant for the decisions by the court in principle before they are made and thereby to influence the court in its decision-making'.[538] Thus, the defendant has the constitutionally guaranteed right to be present in person during the evidence taking by the court and to defend himself.[539] This constitutionally guaranteed position protects the defendant inter alia against so-called in camera hearings where the trial court could take inculpatory evidence in the defendant's absence (more on that below).[540] At the same time, the presence of the defendant at trial is an essential prerequisite for the search of material truth and the culpability principle.[541] The exclusion of the defendant for the protection of state secrets constitutes therefore a serious interference with corresponding defence rights (more on that below).[542]

Moreover, the constitutionally guaranteed right to be heard compels the court to take note of and contemplate the defendant's explanations.[543] This, however, does not preclude ignoring the defendant's request and explanations if there are legitimate formal or substantive reasons for doing so.[544] Furthermore the right to be heard (Art. 103 para 1 Basic Law) requires the court to base its judgment only on facts which the defendant had a chance to comment on. This also includes the possibility to apply for the procurement of evidence closer to the criminal act. However, this does not mean that the right to be heard guarantees the use of only certain evidence or specific types of evidence in criminal proceedings.[545]

Finally, the right to a fair trial is the foundation for the defendant's entitlement to take part in the evidence taking in criminal proceedings. Accordingly, the defendant must be given access to the sources of the established facts. The main standards in this regard are provided by Art. 6 paras 1 and 3 ECHR.[546] The defendant's

---

[538] BVerfG Decision of 16 March 2006, Case no: 2 BvR 168/04, BeckRS 2002, 161311; BVerfG NJW 2016, 1149, 1154; BGH NJW 2010, 2450, 2451; see also *Vogel*, The Core Legal Concepts and Principles, 57; *Stein*, ZStW 97(2)/1985, 314.

[539] BVerfG Decision of 16 March 2006, Case no: 2 BvR 168/04, BeckRS 2002, 161311; BVerfG NJW 2016, 1149, 1154; BGH NJW 2010, 2450, 2451; see also *Vogel*, The Core Legal Concepts and Principles, 57; *Stein*, ZStW 97(2)/1985, 314.

[540] See below IV.C.2.a) General framework.

[541] For more, see BVerfG NJW 2016, 1154; BVerfG NJW 2005, 1641; BGH NJW 2010, 2451; BGHSt 44, 316; BGH NJW 2010, 2451; OLG Hamm Decision of 17 March 2009, Case no: 2 Ss 94/09, BeckRS 2009, 10736; critical on the aspect of duty as not compatible with the right against self-incrimination, *Volk,* Die Anwesenheitspflicht des Angeklagten, 213 – 221; see generally *Stein*, ZStW 97(2)/1985, 303 ff.

[542] See below IV.C.2.b)bb) Witness questioning outside the main hearing.

[543] BVerfG NJW 1979, 414.

[544] BVerfG NJW 1979, 414; BVerfG NJW 1983, 1045; BVerfG Decison 14 Sept. 2010 Case no: 2 BvR 2638/09, BeckRS 2010, 54630; BVerfG NJW 1992, 2811.

[545] BVerfG NJW 1981, 1721.

[546] BVerfG NJW 2007, 205.

right to request evidence during trial is another right that ensures his or her status as participant in the criminal trial with his or her own rights (in compliance with the notion of human dignity).[547] The defendant's right to effectively take part in the inquiry into the material truth by applying for evidence taking corresponds to the safeguarding of justice, which requires not only to adhere to the culpability principle but also to search for material truth and the court's duty to do so ex officio.[548]

Even though the above-outlined principles safeguard the defendant's position in the criminal trial to a certain degree, these principles must still be specified. In fact, the Federal Constitutional Court leaves this duty to the legislature, notably to further specify the requirements of the procedural rights to be heard and to a fair trial. The courts are also entitled to operationalize this right in specific situations.[549] One such example is the jurisprudence of the Federal Court of Justice holding that a trial court can drop a case if the defendant's access to evidence was excessively restricted for reasons of protection of state secrets.[550]

#### bb) Statutory framework

The German CCP enshrines the defendant's right to request to adduce or procure evidence that can serve as proof of facts relevant for guilt or innocence and for sentencing and that enables the defendant to influence the court's decision-making processes.[551] As long as there are no statutorily enumerated reasons on which the court can deny the request, the defendant's request for evidence compels the court to implement it.[552] The defendant's right to apply for the procurement of evidence is further restricted by the Federal Supreme Court's jurisprudence holding that a request for evidence must be sufficiently specific with regard to the evidence in question and the circumstances the evidence in question is expected to mirror; in case of witness evidence, how the witness gained his or her knowledge, and a declaration of what his or her statements should prove.[553] If a motion fails to meet these requirements, the court is not compelled to comply with it. Instead, it is merely a suggestion for the court to focus its inquiry in a given direction and it is in its

---

[547] On the constitutional foundations of this right, see *Perron*, ZStW 108(1)/1996, 131; *Klesczewski*, HRRS 1/2004, 14; *Basdorf*, StV 1995, 310.

[548] BVerfG NJW 2010, 593.

[549] BVerfG NJW 2013, 1060; BVerfG NJW 1992, 2811; BVerfG NJW 1981, 1722.

[550] For more, see below IV.C.3. Dropped Cases over Withheld Evidence.

[551] *Perron*, ZStW 108(1)/1996, 133; Gössel, ZIS 14/2007, 558.

[552] See §§ 244 paras 3 ff.; see also BVerfG NJW 1983, 1054; BVerfG NJW 2010, 593; *Huber*, JuS 2017, 634; *Ventzke*, StV 2009, 655; *Becker*, NStZ 2006, 495; *Klesczewski*, HRRS 1/2004, 10.

[553] BGH NStZ 2006, 586; BGH NJW 2008, 3447; on the constitutionality of this jurisprudence, see BVerfG NJW 1997, 999–1000; for more, see *Beulke*/*Satzger*, JZ 20/1993, 1014; *Jahn*, StV 2009, 663 f.; compare, however, *Perron*, ZStW 108(1)/1996, 135 f.

discretion to refrain from doing so.[554] Even if the defendant's application is in order, the right to request evidence is not absolute.[555] The court may reject the defendant's request, inter alia to procure what is called non-present evidence

- if the taking of evidence is not practicable for legal or factual reasons (i.e. inadmissible or unobtainable),
- if the taking of evidence is not relevant to the court's decision because the evidence aims to prove
  - a fact of common knowledge,
  - a fact that has already been proved,
  - a fact that is wholly inappropriate for a proof, or
  - an exonerating fact that the court can treat as if it were true, or
- if the submission of an evidence request constitutes a misuse of power, namely to protract the proceedings (§ 244 para 3 CCP).[556]

Inadmissibility and unobtainability as grounds for refusal are particularly significant when it comes to defence requests to procure intelligence information or other evidence the authorities are not willing to disclose (more on that below).[557] Furthermore, the court may reject the application to examine a witness who must be summoned from abroad if it, 'in the exercise of its duty-bound discretion, deems the inspection not to be necessary for establishing the truth' (§ 244 para 5 CCP).[558] However, the scope of this restriction requires further clarification, because, as regards the examination of witnesses, criminal courts in Germany must take Art. 6 para 3(d) ECHR in account, which has become considerably influential in legal practice.[559] In affording this right, the courts follow the so-called three step-test of the ECtHR. They consider whether (1) there is good reason for the witness not to appear (at trial) and thus for the admission of his or her testimony in evidence, whether (2) the statements of the absent witness are expected to be the sole or deci-

---

[554] BGH Decision 11 Apr. 2013, Case no: 2 StR 504/12, HRRS 2013 no 611; for more, see *Fezer*, HRRS 11/2008, 457–459; *Basdorf*, StV 1995, 315 ff.

[555] *Gössel*, ZIS 14/2007, 560 f.

[556] *Frister*, ZStW 105(2)/1993, 352; *Gössel*, ZIS 14/2007, 561 f.; on the criterion of non-relevance, see BVerfG Decison 14 Sept. 2010 Case no: 2 BvR 2638/09, BeckRS 2010, 54630; on the misuse of the right to apply for procurement of evidence, see BVerfG NJW 2010, 593.

[557] See below IV.C.2.a) General framework.

[558] On the constitutionality of this provision, see BVerfG NJW 1997, 999–1000; on the rejection of an application to examine a witness from abroad, see BGH Decision 2 May 2018, Case no: 3 StR 355/17, HRRS 2018 no 476; on expert evidence, see also BVerfG NJW 1992, 2811–2812; on other reasons for rejection by the court, particularly regarding experts and adducement of so-called present evidence, see §§ 244 para 3, 245 StPO; *Klesczewski*, HRRS 1/2004, 11.

[559] Esser, NStZ 2017, 605.

sive basis for the defendant's conviction, and whether there are (3) counterbalancing factors sufficient to overcome the difficulties of the defence resulting from the admission of such evidence and to safeguard the fairness of the proceedings as a whole.[560]

### 2. Protection of State Secrets during Trial

As indicated above, the principles of evidence taking by the court and the rights of defence can be restricted in many ways, including by referring to the protection of state secrets. More specifically, the German CCP entitles the authorities to deny the submission or surrendering of documents, in both cases to prevent the publication of state secrets through criminal proceedings,[561] and to deny certain witnesses the authority to testify in criminal proceedings.[562]

#### *a) General framework*

Information in a file or other written information in possession of a public authority that may be used as evidence in criminal proceedings (and thus in a public hearing) must be submitted to the public prosecutor's office or the court.[563] Similarly, the public prosecutor's office must disclose to the trial court the entire evidentiary basis of its allegations against the defendant.[564] The CCP provides in § 96 an exception to these general rules:

> Submission or surrender of files or other documents officially impounded by authorities or public officials may not be requested if their highest superior authority declares that publication of the content of these files or documents would be detrimental to the welfare of the Federation or of a German Land.[565] [Emphasis added].

Thus, the public authorities or prosecutors may deny a court's request for submission or delivery of documents (§ 244 para 2 CCP) or a request by the defence (§ 244 para 3 CCP) where the publication of these files or documents is declared detrimental to the welfare of the federation or one of the German *Länder* ('non-disclosure at trial stage').[566] The law considers information of that nature generally as state secrets or

---

560 BGH NStZ 2017, 603; for more, see *Arslan*, ZIS 6/2018, 218–228.

561 § 96 StPO.

562 § 54 StPO.

563 § 161 StPO states the general obligation of all public authorities to cooperate with the prosecution; this obligation is extended to the cooperation with the courts; for more, see MüKO/StPO-*Hauschild*, § 96 StPO, at 2.

564 199 para 2 StPO; for more, see BVerfG NJW 1983, 1043–1046; LG Hannover FD-StrafR 2015, 369880; MüKO/StPO-*Hauschild*, § 96 StPO, at 11.

565 Translation by Brian Duffett and Monika Ebinger, available at https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p1647.

566 MüKO/StPO-*Hauschild*, § 96 StPO, at 11.

secrets of the public authorities.[567] As indicated above, the fact that the authority is allowed to deny information is not only a restriction permitted pursuant to statute on the court's duty to search, *ex officio*, for the truth by all means but is also a legal reason to restrict the defendant's right to apply for the procurement of evidence as the evidence would be unobtainable within the meaning of § 244 para 3 CCP.[568]

In most of the cases where the police or the intelligence services conduct secret observations on persons, either by using their own personnel or by asking individuals to work for them,[569] these authorities are reluctant to let these individuals testify in court. Making the observation public might reveal the employee's identity or the involvement of the intelligence services, thus providing insights into their tactics. Likewise, informants frequently do not wish to reveal their identity (and publicize the fact that they work for the police/intelligence services). In fact, the promise to keep their identity secret is frequently a precondition for their work for the intelligence services.[570]

In order to keep an identity concealed, the intelligence services can declare this person withheld as a witness. This can lead to a situation where material witnesses cannot testify in court and the court may not be able to reconstruct the crime. The declaration to withhold a witness is considered possible by applying the aforementioned § 96 CCP to persons and not only to documents.[571] A special regulation governing undercover investigators is § 110b para 3 CCP. The superior authority must declare that making this person's identity public would be detrimental to the welfare of the state.[572] Another possibility available to the intelligence services is not to withhold the witness completely but not to give this person the authorization to testify.[573] This is only possible where the person is an agency employee or for-

---

[567] On the definition of these terms, see *Frisch*, Schutz staatlicher Geheimnisse, 201 ff.

[568] BVerfG NJW 1981, 1722 ff.; *Beulke*/*Satzger*, JZ 20/1993, 1014.

[569] Intelligence service personnel may work as undercover agents, conducting long-term observations of persons. They can also work on a single case only; in that case they are called undercover investigators (Verdeckte Ermittler, see § 110a StPO). Intelligence service employees may also have no special cover and only conduct secret observations. Informants are individuals who work for the agencies and merely provide information (Informant, see no 2.1 RiStBV annex D). Individuals who work for the agencies on a long-term basis in order to investigate crimes are called confidants (Vertrauensperson, V-Person, see no 2.2 RiStBV annex D); for more, see *Beulke*/*Satzger*, JZ 20/1993, 1014.

[570] *Soiné*, NStZ 2007, 247; *Beulke*/*Satzger*, JZ 20/1993, 1013.

[571] MüKO/StPO-*Hauschild*, § 96 StPO, at 8; Eisenberg, Beweisrecht der StPO, 298; *Ellbogen*, Verdeckte Ermittlungstätigkeit der Strafverfolgungsbehörden, 140; *Kühne*, Strafprozessrecht, 528; *Beulke*/*Satzger*, JZ 20/1993, 1014.

[572] The statement of any other authority, such as the public prosecutor's office, which wants to keep the name of an informant confidential, is not relevant to the court (BGH NStZ 2001, 333).

[573] In this regard and for civil servants, § 54 para 1 StPO refers to the civil service law of the federation or the federal states (Länder). The corresponding provisions of this law generally entitle the public authorities to deny their servants the authorization to provide

mally committed to keep his or her work for the agency secret. Before accepting the refusal, the criminal court must investigate whether there is no other way to protect the witness. But again, the court's options are limited if the intelligence services provide a plausible explanation for their refusal. In this case, as in cases of withholding documents and witnesses, the superior authority can influence the court's selection of evidence.

The German Federal Constitutional Court has accepted that an endangerment of the health, life, and liberty of the potential witness is grounds to justify not revealing the witness's identity.[574] It is equally accepted that the promise to keep an individual's identity secret or the need to use the person for further secret observations are grounds for withholding the person as a witness.[575]

The declaration must be given by the highest superior authority. The fact that the authority in possession of the document declares to withhold it is not sufficient. To that extent there is some internal control by involving higher ranking officials.[576]

Under § 96 CCP the authorities can withhold documents (including names or statements of witnesses, records of conversations, or images from observations) by claiming that their publication would be detrimental to the welfare of the state,[577] in other words that they are state secrets. Yet, German courts have clarified that it is not enough for the intelligence services to simply claim that the publication of documents might endanger their work and public security. The authority must state facts sufficiently concrete to enable the court to understand the authority's decision.[578] The fact that documents are relevant to the work of the intelligence services in general does not suffice to deny their production.[579] Similarly, the constitutional court has made it clear that it is not enough for the authority to claim the existence of a threat to the welfare of the state.[580] The criminal court must investigate the grounds for withholding the witness and must evaluate whether other means are available to protect the witness.[581] But as long as the intelligence services provide

witness testimony in a court trial if testifying would be detrimental to the welfare of the federation or of a federal state (Land) or seriously endanger or substantially hamper the performance public duties; for more, see BVerfG NJW 1981, 1973; see also *Frisch*, Schutz staatlicher Geheimnisse, 203; MüKO/StPO-*Percic*, § 54 StPO, at 4 ff.; SK/StPO-*Rogall*, § 54 StPO, at 18 ff.

574 BVerfGE 57, 250; see also *Frisch*, Schutz staatlicher Geheimnisse, 217; *Kudlich*, JuS 2004, 929; *Beulke*/*Satzger*, JZ 20/1993, 1015.

575 *Eisenberg*, Beweisrecht der StPO, 299; *Ellbogen*, Verdeckte Ermittlungstätigkeit der Strafverfolgungsbehörden, 146.

576 MüKO/StPO-*Hauschild*, § 96 StPO, at 12.

577 More on the notion of 'welfare of the state', see SK/StPO-*Rogall*, § 54 StPO, at 59 ff.

578 BVerwGE 75, 1 and BVerfGE 57, 250 = NJW 1981, 1719.

579 BVerwGE 75, 1.

580 BVerfGE 57, 250; for more, see *Frisch*, Schutz staatlicher Geheimnisse, 210 ff.

581 BGH StV 1989, 284; BGH NStZ 2005, 43.

plausible arguments, the court has no possibility to challenge their decision.[582] In the end it is the intelligence services (and not the criminal court) who decide whether a witness is allowed to testify.[583]

If the authority does not wish to withdraw its decision, the court cannot use the document(s) in the criminal proceeding. Also, the court must ascertain whether other options than withholding the document are available, such as redacting names or accepting a report by the intelligence services. In fact, in case of a report the services enjoy a great deal of flexibility to conceal the sources of their information as the reports are mostly made up of assertions, presumptions, and publicly available information.[584] But the alternatives are limited, in particular in terms of documentary evidence, as '*in camera*' proceedings, for example, are not allowed in criminal trials.[585] An *in camera* hearing would not only allow the trial court to review whether the non-disclosure decision by an administrative body is justified but would also enable the court to avoid losing evidence relevant to the search for the truth. However, at the same time, the *in camera* hearing would violate the constitutionally guaranteed right of the defendant to be heard, because he or she would not be in a position to defend him- or herself with regard to evidence only disclosed to the trial court.[586] More importantly, with regard to the undisclosed evidence in criminal proceedings, the principle of *in dubio pro reo* applies in favour of the defendant. If the undisclosed evidence is inculpatory, the absence of an '*in camera*' hearing benefits the defendant.[587] In case of witness evidence, witness protection can be afforded by a broad spectrum of measures, which will be explained below.

The court cannot take legal measures against an authority's refusal.[588] The only exception is where the refusal to produce documents is obviously illegal. In that case a court can order the seizure of the documents.[589] The defendant is entitled to challenge the legality of the refusal before the administrative court.[590]

---

582 BVerfG NJW 1981, 1973.

583 On this, see also SK/StPO-*Rogall*, § 54 StPO, at 34 f.

584 On the use of intelligence reports (Behördenzeugnisse) see BGH Decision 26 March 2009 Case no: StB 20/08, HRRS 2009 no 550, at 31.

585 BGH NStZ 2000, 265; BVerfG NJW 2000, 1178; BVerfG NStZ-RR 2013, 379–380 (search warrant based on undisclosed evidence); MüKO/StPO-*Hauschild*, § 96 StPO, at 16; SK/StPO-*Rogall*, § 54 StPO, at 70 ff.; on the use of the so-called *in camera* hearing in administrative court proceedings in Germany, see *Vogel*, ZIS 1/2017, 31 f.; see also BVerfG NJW 2000, 1175–1179; BVerfG NVwZ 2006, 1041–1049; critical, SK/StPO-*Wohlers*/*Greco*, § 96 StPO, at 33.

586 BVerfG NJW 1981, 1974; see also *Frisch*, Schutz staatlicher Geheimnisse, 213; *Vogel*, ZIS 1/2017, 31.

587 BVerfG NJW 2000, 1178; see also BVerfG NStZ-RR 2008, 17.

588 BGHSt 32, 115; MüKO/StPO-*Hauschild*, § 96 StPO, at 19.

589 BGHSt 38, 237.

590 For more, see Frisch, Schutz staatlicher Geheimnisse, 213 f.; MüKO/StPO-*Hauschild*, § 96 StPO, at 19; *Marsch*, Germany, 109.

Yet, neither the court asking the authority to reconsider its decision nor the accused questioning the decision in an administrative proceeding are very likely to be successful. The intelligence services have discretion in deciding what shall prevail: the interest to keep information secret or to conduct criminal proceedings.[591] As long as the intelligence services provide some plausible arguments for their decision, the documents will not be submitted to the courts. Thus, the intelligence services (and not the court or the defence) exercise considerable influence on a criminal trial as they can decide what type of evidence cannot be used.

### *b) Witness protection measures*

As indicated above, a court can take various measures to protect a witness and thus enable the witness to testify in court.[592] Several levels of protection are possible. At the first level the court must examine whether the witness can be protected in the courtroom during the public main hearing. If this is not possible, the court must attempt to question the witness outside the main proceedings by a judge. As a last option the court has to examine whether a written statement by the witness can be accepted as evidence or whether the officer questioning the witness can be heard as a hearsay witness.

These protection measures are in conflict not only with the court's duty to extend the search for the truth to all available facts but specifically also with the defendant's right to examine a witness according to Art. 6 para 3 lit. d ECHR, which requires that the following conditions be met:

(1) the defendant must be informed about the identity of any prosecution witness;

(2) the personal appearance of the witness for examination in trial must be secured;

(3) the defendant must be enabled to follow the examination of the witness acoustically and visually, and

(4) the defendant needs to obtain the opportunity to question the witness and to challenge his or her testimony.[593]

#### aa) Protection during the main hearing

During the main hearing the court can apply different measures to protect a witness. The possibility not to reveal the place of residence provides the least protec-

---

[591] See BVerfGE 57, 250; BGHSt 44, 107; for the practice of administrative courts, see OVG Münster NJW 2015, 1977–1978; VGH Hessen StV 1986, 52–54.

[592] *Ellbogen*, Verdeckte Ermittlungstätigkeit der Strafverfolgungsbehörden, 190; *Kühne*, Strafprozessrecht, 529; *Frisch*, Schutz staatlicher Geheimnisse, 207 ff.; *Soiné*, NStZ 2007, 247.

[593] For more, see *Arslan*, ZIS 6/2018, 219; see also BVerfG NJW 1981, 1973; *Vogel*, ZIS 1/2017, 28 ff.

tion in the main hearing.[594] Not revealing the identity or just giving an old or fake identity provides more protection.[595] But the person is still visible in the courtroom, and the accused or a member of the audience could subsequently identify him or her. The CCP, however, allows to remove the accused from the courtroom if there is a concrete threat to the health of a witness.[596] In this case the accused still gets to know the identity of the witness, which means that this measure only makes sense where the witness is intimidated by the accused. One more step is to exclude the public, which requires a threat for the life, liberty, or freedom of the witness.[597] In this case the accused also gets to know the identity of the witness. Similar problems arise where the witness is interviewed outside the courtroom by video conferencing[598] or where the video of an earlier questioning is shown.[599]

In sum, all these possibilities are no guarantee that the identity of a person is kept secret enough not to be recognized outside the courtroom.[600] In fact, this is the reason why the intelligence services are not likely to accept such low levels of protection.

A higher level of protection is reached if the identity of the witness is kept secret and his or her outer appearance is changed, such as by wearing a wig. The modern version of this camouflage is the visual and acoustical shielding of the witness. The Federal Court of Justice (BGH) allowed this possibility in 2003.[601] In that case the witnesses were placed in a separate room and their testimony was transmitted to the courtroom. A special lens made it impossible to recognize the face; a sound equalizer made it impossible to recognize the voice. These precautions enabled the court to hear the witnesses; otherwise, the ministry as the superior authority would have withheld them on grounds of protection of state secrets in keeping with §§ 54, 96 CCP. The disadvantages of this measure are that the defendant is not only not informed about the real identity of his or her accuser but is also unable to observe the witness's demeanour during the examination.[602] The advantage is that the person can be partially seen and heard in action and can be directly questioned by the prosecution, the court, and the defence.[603] Moreover, the defence has the same level

---

[594] § 68 para 2 StPO; BVerfG NJW 1981, 1974.

[595] § 68 para 3 StPO; BVerfG NJW 1981, 1974.

[596] § 247 StPO, see BGHSt 32, 32.

[597] § 172 GVG; BVerfG NJW 1981, 1974; see also *Frisch*, Schutz staatlicher Geheimnisse, 207; MüKO/StPO-*Percic*, § 54 StPO, at 24.

[598] §§ 247a StPO.

[599] § 58a StPO.

[600] *Soiné*, NStZ 2007, 247.

[601] For more, see BGH NJW 2003, 74; see also BGH NStZ 2005, 43.

[602] ECtHR, Judgment of 20 Nov. 1989 – 11454/85 (Kostovski v. The Netherlands), § 42; ECtHR, Judgment of 10 Apr. 2012 – 46099/06, 46699/06 (Ellis, Rodrigo and Martin v. The United Kingdom), § 74.

[603] *Safferling*, NStZ 2006, 75.

of knowledge with regard to witness testimonies as the court. This type of protection seems to be suited to all cases except those where the mere statement by the witness would reveal his or her identity. Nevertheless, it also leads to the use of 'indirect evidence' in criminal proceedings.

bb) Questioning of the witness outside the main hearing

If the protection of the witness during the main hearing is not possible, the court must attempt to question the witness outside the public proceedings and then introduce the written record of the questioning in the main hearing.[604] The court can only proceed in this way if it has procured a statement by the superior authority to the effect that, in any other case, the witness will be withheld, as the protection of state secrets according to §§ 54, 96 CCP could not be afforded otherwise.[605] The witness may be examined by a commissioned judge (a judge of the court conducting the main proceedings) or a requested judge (a judge of another court asked to do the questioning by judicial assistance). The examination is not public. If the witness will only give evidence if neither the accused nor the defence is present, the court can refrain from notifying the defence and the accused.[606]

The Federal Court of Justice as well as the Federal Constitutional Court have also accepted that the defence can even be excluded from questioning if the authorities would otherwise withhold the witness.[607] On the one hand this enables the court to question the witness at least through a commissioned or requested judge, but on the other hand it restricts the influence of the defence, as the defendant neither knows who the witness is, has no the chance to see and hear the witness during the examination, nor ask questions directly. Furthermore, there is no guarantee that the defendant will later have the same level of knowledge with regard to the witness testimonies as, say, the commissioned judge, who will take part in forming the judgment. Therefore, this measure not only appears to simply lead to the use of 'indirect evidence' in criminal proceedings but also to a quasi *in camera*-hearing and to the potential to produce 'undisclosed incriminating evidence'.[608] The juris-

---

604 So-called Kommissarische Vernehmung, § 223 StPO.

605 BGH NJW 1984, 65.

606 § 224 StPO.

607 BVerfGE 57, 250; BGH NJW 1980, 2088; in a later decision the BGH ruled that if the defence nonetheless gets to know the date and place of the examination and shows up, the defence does have the right to participate in the questioning (BGHSt 32, 115). Insofar not all details have been clarified yet.

608 In fact, under certain conditions, the ECtHR also seems to accept witness hearings in camera, ECtHR, Judgment of 12 Dec.2013 – 19165/08 (Donohoe v. Ireland), § 88; however, compare ECtHR, Judgment of 22 July 2003 – 9647/98 40461/98 (Edwards and Lewis v. The United Kingdom), § 58; ECtHR, Decision of 05 Feb. 2013 – 31777/05 (O'Farrell and

prudence of both federal courts seems to suggest that such a quasi *in camera*-hearing is not categorically denied, whereas both courts strictly oppose an *in camera*-hearing on documentary evidence entirely withheld by the other authorities as state secret, but would principally disclose it to the trial court, provided the defence is excluded from the hearing.[609] However, as a result of the new and accepted option to protect a witness by means of visual and acoustical shielding, there will be fewer questionings outside the main hearing in future.[610]

Witness questioning outside the main hearing not only contravenes the defendant's right to examine a witness under Art. 6 para 3(d) ECHR but also the defendant's right to attend and be present at the main hearing.[611] However, under current law, predominantly opposing interests, namely the interest in clarifying the facts, may exceptionally justify a restriction on the accused's right to attend the main trial.[612]

cc) Written statements and hearsay witnesses

If the aforementioned measures do not guarantee enough secrecy for an individual, the intelligence services will either withhold the witness by a declaration according to § 96 CCP or by a denial of the authorization to testify according to § 54 CCP. In either case the court cannot hear the witness in person. But the court does have the possibility to introduce a witness statement indirectly.[613] As indicated above, both the constitutional requirements of criminal proceedings as well as the statutory framework allow the use of 'indirect evidence'. If a witness is prevented from appearing at the main hearing for an indefinite period of time, the testimony may be replaced by a written statement. Withholding the witness for reasons of secrecy has been accepted as a constellation covered by § 251 para 1 no 2 CCP, namely as unobtainable evidence.[614] In such a case written statements of the witness may be read out in the main hearing. If a written statement of the witness is not available, the courts have also allowed introducing summaries of witness statements compiled by the intelligence services.[615] It is obvious that the defendant's right to examine a witness under Art. 6 para 3(d) ECHR is significantly re-

---

others v. The United Kingdom), §§ 54 and 61; ECtHR, Decision of 10 Jan. 2017 – 40/14 (Austin v. The United Kingdom), § 59; see also *Vogel*, ZIS 1/2017, 32.

609 Critical on that *Vogel*, ZIS 1/2017, 35; compare *Marsch*, Germany, 108.

610 *Safferling*, NStZ 2006, 75.

611 *Frisch*, Schutz staatlicher Geheimnisse, 206.

612 BVerfG Decision of 16 March 2006, Case no: 2 BvR 168/04, BeckRS 2002, 161311; for exceptions see BGH NJW 2010, 2451; see also OLG Hamm Decision of 7 March 2009, Case no: 2 Ss 94/09, BeckRS 2009, 10736.

613 SK/StPO-*Wohlers*/*Greco*, § 96 StPO, at 43; *Ellbogen*, Verdeckte Ermittlungstätigkeit der Strafverfolgungsbehörden, 216; *Kühne*, Strafprozessrecht, 530.

614 BGHSt 29, 109 = NJW 1980, 464; BVerfGE 57, 250; see also *Kudlich*, JuS 2004, 930.

615 See BGH NJW 2007, 384; OLG Hamburg, NJW 2005, 2326.

stricted in such cases. Not only the witness's identity and appearance remain hidden, but any further questioning of the witness is impossible. Still, even such an extensive restriction can be justified.[616]

Another possibility is to question the person who interrogated the witness. The interrogator is a witness him- or herself, so there is no direct conflict with § 250 CCP. However, the interrogator can only present hearsay evidence about the crime and can only provide 'indirect evidence'. A hearsay witness is allowed as long as the original witness (the preferred type of evidence) is not available.[617] Although the interrogator can be questioned in person it is not possible to elicit many details the original witness might have provided. Thus, this presents similar problems as those that occur by introducing written statements.

The courts allow the possibility of introducing 'indirect evidence' of a witness only if the authority's refusal to permit him or her to testify (§ 54 CCP) was not obviously illegal.[618] This can be the case if the publication would not be detrimental to the welfare of the state or if the superior authority fails to provide any reasons for the refusal, if the reasons are not sufficiently substantive, or if the authority provides an arbitrary reason. The Federal Court of Justice has not yet heard a case on point. Only some lower courts have refused indirect evidence on these grounds.[619] Although there are a few examples, it should be noted that the threshold is so high that the non-admission of indirect evidence will rarely happen as long as the intelligence services provide some reasonable grounds for withholding a witness.

The permission of 'indirect evidence' does not mean that the evidence is of the same value as the oral witness statement.[620] The court's duty to search *ex officio* for the material truth (§ 244 para 2 CCP) requires to be especially careful with hearsay evidence even though the court is not bound by any evidence rules as it is allowed to form its conviction freely (§ 261 CCP).[621] However, the court must be more critical than usual and analyze in detail the consistency of indirect evidence. Most importantly, a conviction can never be based on 'indirect evidence' alone, especially if the court receives only summaries of witness statements compiled by the intelli-

---

[616] ECtHR, Judgment of 28 Feb. 2016 – 51277/99 (Krasniki v. The Czech Republic), § 75 ('Article 6 does not grant the accused an unlimited right to secure the appearance of witnesses in court'); for more see *Arslan*, ZIS 6/2018, 214 f.

[617] BVerfGE 57, 250; BGH NStZ 2000, 265; BGHSt 32, 115; see also *Droste*, Handbuch des Verfassungsschutzrechts, 597.

[618] BGHSt 29, 109.

[619] See *Eisenberg*, Beweisrecht der StPO, 301; *Ellbogen*, Verdeckte Ermittlungstätigkeit der Strafverfolgungsbehörden, 237.

[620] *Ellbogen*, Verdeckte Ermittlungstätigkeit der Strafverfolgungsbehörden, 256; BVerfG NJW 1981, 1722.

[621] BVerfG NJW 1981, 1722.

gence services. 'Indirect evidence' must always be backed by other, direct evidence.[622] According to § 261 CCP, the evaluation of evidence by the court must be described in detail in the judgment (§ 260 para 4 CCP). The judgment must highlight that the court was aware and did pay special attention to the uncertainties of the 'indirect evidence'. If there are doubts about facts for or against the accused, the court is compelled to strictly apply the principle of deciding in favour of the accused (*in dubio pro reo*). This is particularly so where withheld evidence could be in favour of the accused. The Federal Court of Justice has explicitly highlighted that the interest of the state to keep information secret may not lead to disadvantages for the rights of the accused.[623]

In the final analysis, German courts attempt to compensate for the reduced value of 'indirect evidence' by being particularly careful in assessing it. The rationale behind this approach is that some evidence is better than no evidence at all.[624] But in many cases the court will not really be in a position to assess the value of the evidence, because it lacks necessary information, such as the circumstances involved in gathering the evidence, the motivation of the witness at the time, and, especially, because of omissions in the statements. This is equally true for the defence, which makes it almost impossible to question or counter such evidence. To this extent 'indirect evidence' can only support the court's reasoning based on other evidence.

### 3. Dropping Cases over Withheld Evidence

If material evidence is withheld by the authorities ('non-disclosure'), for instance by the intelligence service, the question arises whether the court may drop a case because a fair trial is not possible. The Federal Court of Justice has decided that this is a possibility.[625] In the case at issue the accused (*Mounir el Motassadeq*) was indicted for aiding one of the September 11 (*Mohamed Atta*) hijackers. One witness (*Ramzi Binalshib*) who might have clarified the involvement of the accused in the crime was imprisoned in the U.S. and not allowed to be questioned by the court. An FBI officer interrogated in court was not allowed by the FBI to give evidence on statements made by *Binalshib*. Information on statements by *Binalshib* in the possession of the German intelligence services was withheld. The Federal Court of Justice ruled that the 'non-disclosure' of evidence of such importance violates the fair trial rights of the accused. The court stated that if, as a result of the evidence withheld, the judge has only a minimum of facts as a basis for deciding the case,

---

622 BGH NStZ 2000, 265; see also BGHSt 49, 112.

623 BGHSt 49, 112; see also BGH NStZ 2000, 265; BVerfGE 57, 250; *Kudlich*, JuS 2004, 930; *Beulke*/*Satzger*, JZ 20/1993, 1014 f.

624 See BVerfGE 57, 250.

625 BGHSt 49, 112.

the case must be dropped. Yet, in the case of *el Motassadeq* the court saw other means to compensate for the violation of the fair trial right. It ordered a rehearing of the case at the first instance court. Concerning the evidence, the first instance court was ordered to be particularly careful in considering the evidence and to strictly decide *in dubio pro reo*. In the rehearing, U.S. authorities provided new evidence which facilitated (together with other evidence) proof of *el Motassadeq*'s involvement in the attacks of September 11.[626]

### 4. Inadmissible Evidence

If evidence gathered by the intelligence services is introduced into a criminal proceeding, the evidence is not necessarily admissible for proving the guilt of the accused. German law recognizes that the search for the truth must not be pursued at any price and, accordingly, the court's duty and power to 'extend the taking of evidence to all facts and means of proof relevant to the decision' (§ 244 para 2 CCP) must be restricted.[627]

In terms of the question whether a piece of evidence can be used as a basis for a criminal conviction, the German criminal procedure system distinguishes between prohibitions to take evidence (*Beweiserhebungsverbote*) and inadmissibility of (improperly obtained) evidence (*Beweisverwertungsverbote*). Violations during evidence gathering may result in an inadmissibility of the evidence in court. Yet the courts have allowed many exceptions to this rule and unfortunately not succeeded in developing a coherent system governing the admissibility of evidence.[628] In the context of intelligence service information in criminal proceedings, two constellations are of special interest: (1) the gathering of evidence without the necessary legal basis, (2) the use of information collected abroad.

#### *a) Illegally collected evidence*

The collection of evidence by the intelligence services can be illegal for a number of reasons.[629] The intelligence services may lack the authority to investigate certain crimes, such as the investigation of tax crimes in the above-mentioned *Liechtenstein* case.[630] The services may also lack the authority for certain coercive measures such as computer searches via the internet. And the services may have

---

626 See BGH NJW 2007, 384.

627 For more, see above IV.C.1.a)aa) Constitutional framework.

628 See for the developments in recent years, *Fezer*, JZ 2007, 665 ff. and 723 ff.; *Jahn*, Beweiserhebungs- und Beweisverwertungsverbote, C39.

629 *Greßmann*, Nachrichtendienste und Strafverfolgung, 417 f.; *Lang*, Geheimdienstinformationen, 120 ff.

630 See *Schünemann*, NStZ 2008, 305; *Sieber*, NJW 2008, 881 f.; *Trüg*, NJW 2008, 887.

disregarded the principle of proportionality and not turned to less far-reaching measures.

Violations do not necessarily prohibit the evidence from being admitted in court.[631] The Federal Court of Justice attempts to balance the public interest in prosecuting crimes with the interest of the individual not to be infringed in his or her rights. Major factors in judging admissibility are the seriousness of the crime and the seriousness of the violation of rights by the intelligence services.[632] The more serious the violation by the services, because they do not just violate a formal regulation of the CCP but infringe on important basic rights in the constitution, the more likely the courts will not admit the evidence in the main hearing.

A special problem arises if the intelligence services gather illegally collected evidence. This may occur when the intelligence services ask individuals to work for them, say as informants or confidants. Courts generally do allow evidence illegally collected by individuals.[633] An exception can be made where the conduct of the individual may be attributed to the intelligence services.[634] Therefore, admissibility depends very much on the question whether the individual acted on his or her own initiative or whether he or she was instructed by the intelligence services. However, even if the conduct of the individual is attributed to the intelligence services the courts tend to strike a balance between the interest of the prosecution and individual rights,[635] thus allowing the rules of evidence and procedure to be 'bypassed'.

As already indicated above, the measures of the intelligence services frequently do not produce the evidence later used in court but only provide leads for further investigations by the police or the prosecution ('indirect evidence' at investigation stage).[636] If the evidence gathering by the intelligence services was illegal, the question of what happens with the evidence subsequently legally produced by the police, prosecution, or court arises only if respective evidence is taken in the main hearing. This procedural question may never come up, especially if the prosecution authorities do not disclose the existence of corresponding evidence ('undisclosed incriminating evidence' at investigation stage) and if they obtain further evidence by using the illegally gathered evidence. In this regard, it must be noted that the

---

631 See BVerfG NStZ 2006, 46; *Jahn*, Beweiserhebungs- und Beweisverwertungsverbote, C32; *Arslan*, Aussagefreiheit des Beschuldigten, 365.

632 See BGHSt 31, 304; BGHSt 38, 14; BGHSt 47, 172; BGH NJW 1997, 1018; BGH NJW 2013, 2271; *Jahn*, Beweiserhebungs- und Beweisverwertungsverbote, C45.

633 BGHSt 36, 172; *Eisenberg*, Beweisrecht der StPO, 116; LR/StPO-*Gleß*, § 136a, para 10; *Jahn*, supra note 632, C100; *Sieber*, NJW 2008, 886.

634 *Eisenberg*, Beweisrecht der StPO, 118; *Jahn*, Beweiserhebungs- und Beweisverwertungsverbote, C101.

635 BGHSt 40, 211.

636 See above IV.B.4. Use of Intelligence Information.

German system, in principle,[637] does not recognize the 'fruit of the poisonous tree doctrine'.[638] As a result, the courts, again, balance the interests of the prosecution against individual rights. There are not many cases where evidence was not allowed in court. The most prominent example is the case where the court disallowed evidence collected by the prosecution based on illegal information gathered by the intelligence services.[639] Because the intelligence services violated the important right of privacy of correspondence, posts, and telecommunication (Art. 10 Basic Law), the court regarded the violation as sufficiently grave not to admit the evidence in question. But even in this case the prohibition was not total as the court allowed the use in cases of serious crime.

Thus, evidence illegally collected by the intelligence services will not automatically be banned from being used in a criminal proceeding. This will only be the case where the intelligence services gather evidence regarding minor crimes for which they are not responsible. If they collect information about serious crimes enumerated as falling within the scope of their duties, the evidence is likely to be allowed in the proceeding. In short, one can say that German jurisprudence puts more emphasis on facilitating public prosecutions and less on protecting individual rights.

### *b) Evidence collected abroad*

In recent years the intelligence services have been receiving more and more information from abroad. The intelligence services, the police, and the prosecution see no problem in using such information as a basis for further investigations in Germany. German authorities take this approach even if the information may have been collected by illegal means such as torture.[640] This scenario is rarely made public because, as already emphasized above, in many cases only the outcomes of additional investigations are used as evidence in court.[641]

In more and more cases the collection of evidence abroad itself is important when the crime is committed in a transnational setting. Examples are terrorist attacks where the planning and training of at least some members of a group take place outside the countries where the attacks are committed. Another example are the criminal acts of the so-called returnees from the war in Syria, who face criminal

---

637 On the exception with regard to information concerning the so-called core area of privacy, see BVerfG NJW 2016, 1787.

638 *Sieber*, NJW 2008, 886; *Arslan*, Aussagefreiheit des Beschuldigten, 371; *Eisenberg*, Beweisrecht der StPO, 118; *Jäger*, Christian, Beweisverwertung und Beweisverwertungsverbote, 111; *Jahn*, Beweiserhebungs- und Beweisverwertungsverbote, C91.

639 BGHSt 29, 244.

640 See *Hetzer*, Kriminalistik 59, 148.

641 See above IV.B.3 Suspending a Transfer and 4. Use of Intelligence Information.

investigation in Germany. These cases raise the question whether evidence collected abroad can be used in court.[642] The main issue in such cases is what standards should apply for introducing evidence into a German criminal proceeding. The courts have clarified that, for purposes of evidence gathering, the relevant standards are the standards of the country in which the interrogation or the coercive measures take place.[643] Hence, German courts will examine in each case whether the evidence was collected in compliance with the foreign standards.[644]

Yet, the examination whether the collection of evidence was legal according to foreign standards is only a precondition to the question whether the evidence is admissible. The ultimate question of admissibility is answered according to German law.[645] Therefore, illegally collected evidence does not necessarily mean that the evidence is not allowed in court. This is only the case if the breach of foreign law is also relevant under German standards. Conversely, the legal collection of evidence abroad does not mean that the evidence is allowed if German standards do not allow such collection. This can be the case where German authorities initiate an interrogation abroad and the interrogation techniques used are not allowed in Germany.[646] Evidence can be disallowed without the involvement of German authorities if the German standards of rule of law (*rechtsstaatliche Anforderungen*) were not observed.[647]

The question whether the rule of law standards had been observed was discussed in the proceedings against *Mounir el Motassadeq* on terrorism-related charges mentioned above.[648] In this case the U.S. provided summaries of statements of several witnesses imprisoned by the United States. There were doubts whether the statements were obtained without the use of torture, as there had been press coverage concerning these witnesses. From the point of view of the law, measures such as

---

642 The classical mechanisms to obtain evidence are international judicial assistance or mutual cooperation (internationale Rechtshilfe). These aspects will not be examined any further in this context. The assistance can vary greatly especially when EU-countries are asked for help, as there is already an extensive legal network for the exchange of information within the EU or parts of the EU.

643 BGH NStZ 1994, 595; BGH NStZ 1992, 394; see also *Böse*, ZStW 114/2002, 148; *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, 84.

644 BGH NStZ 1992, 394; BGH NStZ 1983, 181.

645 BGH NStZ 1996, 609; *Böse*, ZStW 114/2002, 148.

646 *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, 84; the involvement of German authorities abroad is obviously hard to prove. Information is often kept secret. If information becomes public, it is predominantly too general in nature to be produced in a criminal proceeding. For example, it has become public that German intelligence service agents took part in interrogations in Guantanamo (see *Hetzer*, Kriminalistik 59, 148). Yet, as long as this participation cannot be linked to the interrogation of a specific person, the complaint that a statement was obtained by bypassing German law will be unsuccessful.

647 BGH NStZ 1983, 181.

648 See OLG Hamburg, NJW 2005, 2326.

'waterboarding' may be legal under U.S. law but unquestionably constitute torture under German law.[649] § 136a CCP is quite clear regarding such ill-treatment and completely prohibits any evidence based on this ill-treatment.[650] It is generally accepted that the standards of § 136a CCP must be met in any proceeding abroad.[651]

The problem in the case was that the court, the higher regional court of Hamburg (OLG Hamburg), did not have more than a vague suspicion that the witnesses had been tortured. Neither the U.S. authorities nor the German intelligence services provided any information on the circumstances under which the witnesses had been questioned. The court solved the problem by applying a high burden of proof. As long as there was no proof that the witnesses had been tortured, the court assumed that they were not, and their statements were admissible in court.[652] Thus, the assumption of '*in dubio pro reo*' does not apply where a witness may have been tortured. This ruling is in line with a long-standing point of view of the Federal Court of Justice and was not overruled in the appellate proceeding.[653] *De facto* this means that the defence must prove that the witnesses were tortured if their statements should not be used in court. This is an almost impossible task if the state authorities do not even disclose where the witnesses are held in custody. Thus, once again, German jurisprudence puts public prosecution first and the protection of individual rights second. By demanding high standards of proof for the defence, German jurisprudence is not consistent with the jurisprudence of the European Court of Human Rights.[654]

## Summary

In Germany, security, the protection of the state and the constitutional order, the prevention of danger, and the prosecution of crimes are in many different ways closely linked areas of the law. The theoretical foundations of these elements of domestic security lead to different constitutional requirements for the frameworks of the intelligence services, the police, and the criminal prosecution authorities. Differences in the constitutional foundations for providing domestic security are

---

649 For more, see *Arslan*, Aussagefreiheit des Beschuldigten, 284.

650 Besides § 136a StPO, the court discussed the U.N. anti-torture treaty, to which Germany is a signatory and which is directly applicable in Germany (OLG Hamburg, NJW 2005, 2326). Any evidence based on torture is not admissible in a criminal proceeding (art. 15); more on that, see *Arslan*, ZStW 127(4)/2015, 1133 f.

651 LR/StPO-*Gleß*, § 136a, para 11, 72; *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise, 219.

652 OLG Hamburg, NJW 2005, 2326.

653 See BGH NJW 2007, 384.

654 For more, see *Arslan*, Aussagefreiheit des Beschuldigten, 615.

exacerbating normative tensions, which the Federal Constitutional Court is attempting to resolve by compromise: the Court has accepted the existence of new security threats and the resulting need to reconfigure the security framework. At the same time, the Court has set limits on this transformation. With a view to the fact that the objective is a holistic security paradigm as described in the introduction, the following principles have been constitutionally mandated:

– With regard to the questions on how people behave and to what extent risks might arise as a result thereof: rather than recording human behaviour all round, the aim should be to identify increased risk areas, and rather than addressing all the risks or dangers of a certain type, risks must be selected by relevance. Thus, random observation of everything and everyone is prohibited. Similarly, the Court requires a prohibition of total surveillance, profiling, and the collection of personal data for unspecified purposes. The Court further emphasizes that the legislature is strictly prohibited under the constitution to seek to enable the authorities to comprehensively reconstruct all the activities of a citizen, not least by not tolerating the current practice of allowing the unregulated interconnectivity of already existing databases. In sum, there are risks and dangers which society must accept.
– With regard to questions about the type of risks that actually arise and might be averted and the possible causes of these risks:
  instead of aiming at the complete exposure, prevention, and prosecution of risks, it will be necessary to accept dark numbers. Constitutional jurisprudence clearly states that presumptions or general investigative experiences of competent authorities alone do not suffice as a factual basis for an interference with basic rights and freedoms. Instead of using everything technically feasible, due attention must be paid to the protection of fundamental rights.[655] In line with this, the Court requires, for instance, that the core area of an individual's private life must not be subject to state surveillance.

Most importantly, the Court continues to insist on a separation between the intelligence services, the preventive role of the police, and criminal prosecution, as the proportionality between the social control by the state and its powers of intervention requires a differentiated and balanced approach. However, the customary clear-cut separation between intelligence, the preventive role of the police, and criminal prosecution, which was based on differences in their responsibilities, objectives, and respective *modi operandi*, and especially on different investigation thresholds, has been abandoned in favour of an internal security policy focused on effectiveness. The result, in terms of criminal justice, is that evidence collection, especially by non-criminal authorities, is increasingly becoming a matter of security. As the boundary lines recently drawn by the Constitutional Court between the

---

655 *Gusy*, Polizei- und Ordnungsrecht, 37; see also *Paeffgen*, StV 1999, 676.

intelligence services, the preventive role of the police, and criminal prosecution are quite thin, it remains to be seen to what extent the new normative boundaries between these areas can be respected in practice. Particularly the laws on the transfer of intelligence information and their application in criminal proceedings are quite illustrative in the sense that the laws of intelligence and criminal procedure apply significant restrictions on the principle of informational separation.

Intelligence services in Germany are allowed to render a 'non-disclosure' decision, *inter alia* on grounds of protecting state secrets during criminal investigations. If they do not take such a decision and if the matter involves crimes against the security of the state or crimes of major importance, they may provide intelligence information to the criminal investigation authorities either unsolicited or on request. The issue of whether and to what extent intelligence services may also support the criminal investigation authorities in other areas of crime, *inter alia* by transmitting intelligence information in accordance with their general duty of providing so-called administrative cooperation, is controversially debated.

Even if intelligence is transferred, a direct use of intelligence information by the criminal investigation authorities (and the courts) is only authorized if the information could also have been gathered under the CCP (the so-called hypothetical order). As the investigation is conducted in secret and the prosecutor is allowed to restrict access to the investigation files, the defence will in most cases only be informed about the existence of some inculpatory evidence but not about the fact that this evidence comes from the intelligence services. Thus, the intelligence information will be used as 'indirect evidence' against the defendant already at the investigation stage. The prosecutor, however, is compelled to disclose all the results of his or her investigations, including the origin of the evidence, when filing the indictment in court.

Whereas intelligence law explicitly stipulates the two types of transfer mentioned above (unsolicited or on request), in practice, intelligence information is also shared between the intelligence services and the investigation authorities based on mutual trust. Specifically, the investigation authorities promise not to use the shared information at court in trial (so-called '*nicht gerichtsverwertbare Informationen*'). Moreover, an indirect use of intelligence information as investigative tips and leads, which do not need to be disclosed to the defence, is permitted without complying with the so-called hypothetical order. In both cases intelligence information is used at the investigation stage as 'undisclosed incriminating evidence'.

As regards the trial stage, the CCP entitles public authorities including the intelligence services to render a 'non-disclosure' decision to a criminal court, if the requested evidence (documents or witnesses) must be withheld for the protection of state secrets (similar to the above-mentioned intelligence law). If the evidence withheld is material to the case, the German Federal Court of Justice considers it

feasible to drop the case entirely in keeping with the right to a fair trial. According to the German Constitutional Court, evidence cannot be disclosed to a trial court in a so-called '*in-camera* hearing'. However, this does not mean that the intelligence services and the courts are unable to introduce state secret-related evidence into trial on the one hand and to protect state secrets on the other hand. They can achieve both by submitting an intelligence report. This is how the intelligence services produce 'indirect evidence' at trial. Further, for witness evidence, the German CCP provides a wide variety of witness protection techniques: 'indirect evidence' is used when an anonymous witness is heard at trial with visual and acoustical shielding, the interrogator of an earlier interview with an absent witness is heard as hearsay evidence, or the written statements of an absent witness are read out as documentary evidence. 'Undisclosed incriminating evidence' may be generated by hearing an anonymous witness in the presence of a commissioned judge of the trial court and by excluding the defence.

# References


*Abbe,* Der polizeiliche Staatsschutz und seine Datenbanken. [https://police-it.org/der-polizeiliche-staatsschutz-und-seine-datenbanken].

*Albert*, *Helmut*, Informationsverarbeitung durch Nachrichtendienste am Beispiel der Verfassungsschutzbehörden, in: Guido, Korte/Manfred, Zoller (Hrsg.), Informationsgewinnung mit nachrichtendienstlichen Mitteln: Rahmenbedingungen, Einsatzmodalitäten, Verarbeitungsaspekte. Beiträge zur Inneren Sicherheit, Fachhochschule des Bundes. Oktober 2001. 88–110. [http://www.hsbund.de/SharedDocs/Downloads/2_Zentralbereich/20_Referat_W/50_Publikationen/15_Beitraege_Innere_Sicherheit/band_16.pdf?__blob=publicationFile&v=].

*Alsberg, Max*, Der Beweisantrag im Strafprozess, 6. Auflage. Köln 2013.

*Arslan, Mehmet*, Intelligence and Crime Control in the Security Law of Germany in: The Limits of Criminal Law. Anglo-German Concepts and Principles, ed. by Matthew Dyson and Benjamin Vogel, 2018, Cambridge, 509–537.

– The Right to Examination of Prosecution Witnesses, ZIS 6/2018, 218–228.

– Vorgaben des internationalen Menschenrechtsschutzes für das nationale Strafverfahrensrecht am Beispiel der Selbstbelastungsfreiheit, ZStW 127(4)/2015, 1111–1135.

– die Aussagefreiheit des Beschuldigten in der polizeilichen Befragung. Ein Vergleich zwischen EMRK, deutschem und türkischem Recht. Berlin 2015.

*Arzt, Clemens*, Antiterrordatei verfassungsgemäß – Trennungsgebot tot? NVwZ 2013, 1328–1332.

*Basdorf, Clemens*, Änderungen des Beweisantragsrechtes und Revision, StV 1995, 301–320.

*Becker, Jörg-Peter*, Die Rechtsprechung des BGH zum Beweisantragsrecht, NStZ 2006, 495–499.

*Beulke*, *Werner/Satzger, Helmut*, Zur behördlichen Sperrerklärung analog § 96 StPO. Anm. zum BGH-Beschluss v. 10.2.1993 – 5 StR 550/92 (LG Stade), JZ 20/1993, 1013–1016.

*Böse, Martin*, Die Verwertung im Ausland gewonnener Beweismittel im deutschen Strafverfahren. ZStW 114/2002, 148–182.

*Brodowski, Dominik*, Alternative Enforcement Mechanisms in Germany in: The Limits of Criminal Law. Anglo-German Concepts and Principles, ed. by Matthew Dyson and Benjamin Vogel, 2018, Cambridge, 366–392.

*Brandt, Karsten*, Das Bundesamt für Verfassungsschutz und das strafprozessuale Ermittlungsverfahren. Die Mitwirkung des Bundesamtes für Verfassungsschutz in strafprozessualen Ermittlungsverfahren vor dem Hintergrund des sog. Trennungsgebots. Berlin 2015.

*Bürger, Sebastian*, Unmittelbarkeitsgrundsatz und kontradiktorische Beweisaufnahme, ZStW 128(2)/20016, 518–546.

*Chalkiadaki, Vasiliki*, Gefährderkonzepte in der Kriminalpolitik. Rechtsvergleichende Analyse der deutschen, französischen und englischen Ansätze. Wiesbaden 2015.

*Daun, Anna*, Die deutschen Nachrichtendienste, in: Thomas, Jäger/Anna, Daun, Geheimdienste in Europa. Transformation, Kooperation und Kontrolle. Wiesbaden 2009, 56–77.

*Denninger*, Verfassungsschutz, Polizei und die Bekämpfung der Organisierten Kriminalität, KritV 1994, 232–241.

*Droste*, Handbuch des Verfassungsschutzrechts. 5. Auflage. Stuttgart 2007.

*Dumitrescu*, Das Unmittelbarkeitsprinzip im deutschen und schweizerischen Strafprozessrecht, 130(1)/2018 ZStW, 106–155.

*Eberl*, Kommentar. Immanuel Kant zum ewigen Frieden. Berlin 2011.

*Egbert*, About Discursive Storylines and Techno-Fixes: The Political framing of the Implementation of Predictive Policing in Germany, European Journal for Security Research 3 (2), 95–114, (2018).

*Eisenberg, Ulrich*, Beweisrecht der StPO. Spezialkommentar, München 2006.

*Ellbogen, Klaus*, Die verdeckte Ermittlungstätigkeit der Strafverfolgungsbehörden durch die Zusammenarbeit mit V-Personen und Informanten. Berlin 2004.

*Engelhart, Marc*, Countering Terrorism at the Limits of Criminal Liability in Germany in: The Limits of Criminal Law. Anglo-German Concepts and Principles, ed. by Matthew Dyson and Benjamin Vogel, 2018, Cambridge, 435–465.

– The Secret Service's Influence on Criminal Proceedings. In: A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications/Wade, Marianne/Maljević, Almir (Hrsg.), 2010, Springer, 505–547.

*Esser, Robert*, Verwertbarkeit unkonfrontierter Zeugenaussagen, NStZ 2017, 602– 607.

*Fezer, Gerhard*, Verschärfung des Konnexitätserfordernisses. Anmerkung zu BGH 5 StR 38/08 – Urteil vom 10. Juni 2008, HRRS 11/2008, 457–459.

– Die Rechtsprechung des BGH zum Strafverfahrensrecht seit 1995. JZ 2007, 665–676, 723–729.

– Reduktion von Beweiserfordernissen – Systemverändernde Tendenzen in der tatrichterlichen Praxis und Gesetzgebung, StV 1995, 263–270.

– Tatrichterlicher Erkenntnisprozess – Freiheit der Beweiswürdigung, StV 1995, 95–101.

*Franke, Ulrich*, Öffentlichkeit im Strafverfahren, NJW 2016, 2618–2621.

*Frisch, Wolfgang*, Der Schutz staatlicher Geheimnisse im Strafverfahren, in: Dünyada ve Türkiye'de Ceza Hukuku Reformları Kongresi, Sözüer Adem (Hrsg.), İstanbul 2013, Band 1, 201–230.

*Frister, Helmut*, Das Verhältnis von Beweisantragsrecht und gerichtlicher Aufklärungspflicht im Strafprozess, ZStW 105(2)/1993, 340–363.

*Fromm, Ingo E.*, Zulässige und verfahrensfehlerhafte Beschränkungen des Öffentlichkeitsgrundsatzes im Strafprozess, NJOZ 2015, 1193–1197.

*Gazeas, Nikolaos*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden. Berlin 2014.

*Gercke, Marco*, PRISM, TEMPORA und das deutsche Strafverfahren – Verwertbarkeit der Erkenntnisse ausländischer Nachrichtendienste. Wann nachrichtendienstliche Erkenntnisse an deutsche Strafverfolgungsbehörden weitergeleitet und verwertet werden dürfen. CR 11/2013, 749–754.

*Geismann, Georg*, Kants Rechtslehre vom Weltfrieden. ZphF 37/1983, 363–388.

*Gleß, Sabine*, Predictive policing und operative Verbrechensbekämpfung in: Rechtsstaatlicher Strafprozess und Bürgerrecht. Gedächtnisschrift für Edda Weßlau, Herzog, Felix/Schlothauer, Reinhold/Wohlers, Wolfgang, Berlin 2016, 165–180.

– § 136a in: Löwen-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar. 26. Auflage, 4. Band. Berlin 2007, 580–631.

*Gnüchtel, Ralf*, Das Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus, NVwZ 2016, 1113–1119.

*Gössel, Karl Heinz*, Über die Ablehnung prozessverschleppender Beweisanträge, ZIS 14/2007, 557–564.

*Graulich, Kurt*, Sicherheitsrecht des Bundes – Recht der Nachrichtendienste in Deutschland. Skripte. [http://kaiser.rewi.hu-berlin.de/doc/Vorlesung_3_12.05.2016.pdf.]

– Strafverfolgungsvorsorge. Gegenstand und rechtliche Verortung. NVwZ 2014, 685–691.

*Greßmann, Michael*, Nachrichtendienste und Strafverfolgung in: Handbuch des Rechts der Nachrichtendienste, in: Dietrich, Jan-Hedrik/Eiffler, Sven-R (Hrsg.), Stuttgart 2017, 401–452.

*Griesbaum, Wallenta*, Strafverfolgung zur Verhinderung terroristischer Anschläge – Eine Bestandsaufnahme. NStZ 2013, 369–379.

*Gusy, Christoph*, Polizei- und Ordnungsrecht. 10. Auflage. Tübingen 2017.

– in Schenke/Graulich/Ruthig Sicherheitsrecht des Bundes, BND-Gesetz

– Polizei und Nachrichtendienste im Kampf gegen die Organisierte Kriminalität. KritV 1994, 242–251.

– Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten. ZRP 1987, 45–52.

*Hauschild, Jörn*, StPO § 96 (Amtliche Schriftstücke) in: Münchener Kommentar zur StPO. 1. Auflage. München 2014.

*Hefendehl, Roland*, Die Entfesselung des Strafverfahrens über Methoden der Nachrichtendienste – Bestandsaufnahme und Rückführungsversuch –, GA 2011, 209–231.

*Hermes, Georg*, Besprechung. Der Staat 24/1985, 118–121.

*Hetzer, Wolfgang*, Verschleppung und Folter – Staatsraison oder Regierungskriminalität? Kriminalistik 59, 148–159.

*Huber, Bertold*, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefunisse und Relegungsdefizite, NJW 2013, 2572 – 2577.

*Huber, Michael*, Ablehnung von Beweisanträgen, JuS 2017, 634–637.

*Hütwohl, Mathias*, Die Zentralstelle für Finanztransaktionsuntersuchungen (FIU) – Bekämpfung der Geldwäsche und Terrorismusfinanzierung nach dem neu gefassten Geldwäschegesetz. ZIS 11/2017, 680 –687.

*Isensee, Josef*, Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates. Berlin 1983.

*Jahn, Matthias*, Der Beweistransfer aus dem Ermittlungsverfahren in die Hauptverhandlung nach dem Model des AE-Beweisaufnahme, StV 2015, 778–783.

– Konnexitätsdoktrin und Fristenlösungsmodell – Die verfassungsrecht-lichen Grenzen der Fremdkontrolle im Beweisantragsrecht der Verteidigung durch den Bundesgerichtshof, StV 2009, 663 – 669.

– Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus, Gutachten C für den 67. Juristentag in: Ständige Deputation des Deutsche Juristentags (Hrsg.), Verhandlungen des Siebenundsechzigsten Deutschen Juristentages, pp. C1–C128, München 2008.

– Vorhalt von Urkunden, JuS 2007, 193–194.

*Jäger, Christian*, Beweisverwertung und Beweisverwertungsverbote im Strafprozess. München 2003.

*Jaeckel, Liv*, Gefahrenabwehrrecht und Risikodogmatik. Moderne Technologien im Spiegel des Verwaltungsrechts. Mohr Siebeck. Tübingen 2010.

*Klesczewski, Diethelm*, Das System der Ablehnungsgründe der §§ 244 f. StPO – zugleich ein Beitrag zur Konnexität von Beweismittel und Beweistatsache, HRRS 1/2004, 10–18.

*Korte, Guido*, Informationsgewinnung der Nachrichtendienste mit nachrichtendienstlichen Mitteln. Grenzen und Möglichkeiten der Informationsbeschaffung durch die Verfassungsschutzbehörden in: Guido, Korte/Manfred, Zoller (Hrsg.), Informationsgewinnung mit nachrichtendienstlichen Mitteln: Rahmenbedingungen, Einsatzmodalitäten, Verarbeitungsaspekte. Beiträge zur Inneren Sicherheit, Fachhochschule des Bundes. Oktober 2001. 35–88 [http://www.hsbund.de/SharedDocs/Downloads/2_Zentralbereich/20_Referat_W/50_Publikationen/15_Beitraege_Innere_Sicherheit/band_16.pdf?__blob=publicationFile&v=3].

*Kröpil, Karl*, Wichtige Grundsätze des Strafverfahrens unter Berücksichtigung einiger Aspekte aus dem Strafverfahren gegen Christian Wulff, JuS 2015, 213–218.

*Kudlich, Hans*, Staatliche Geheimhaltung und strafrechtliche Aufklärung – Fall El Motassadeq, JuS 2004, 929–931.

*Kühne, Hans-Heiner*, Strafprozessrecht. 7. Auflage. Heidelberg 2007.

*Lang, Xenia*, Geheimdienstinformationen im deutschen und amerikanischen Strafprozess, Berlin 2013.

*Link, Jochen*, Wahrheit und Gerechtigkeit als Axiome des Strafverfahrensrechts? in: Oglakcioglu, Mustafa Temmuz/Schuhr, Jan/Rückert, Christian, Axiome des nationalen und internationalen Strafverfahrensrechts, Baden-Baden, 2016, 97–120.

*Marsch, Nikolaus*, Country Fiche: Germany, in: European Parliament Study on 'National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges', 106–111. [http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf].

*Meyer-Goßner, Lutz/Schmitt, Bertram*, Strafprozessordnung. Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen. 56. Auflage. München 2016.

*Nehm, Kay*, Das nachrichtendienstrechtliche Trennungsgebot und die neue Sicherheitsarchitektur. NJW 2004, 3289–3295.

*Paeffgen, Hans-Ullrich*, „Vernachrichtendienstlichung" von Strafprozess- (und Polizei-) recht im Jahr 2001. Weitere grundsätzliche Anmerkungen zur deutschen „Sicherheitsrechts"-Entwicklung bis zum Terrorismusbekämpfungs-Gesetz. StV 2002, 337–341.

– Das Urteil des Bundesverfassungsgerichts zum G 10 in der Fassung des Verbrechensbekämpfungsgesetzes 1994. StV 1999, 668–678.

*Papier, Hans-Jürgen*, Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft. NJW 2017, 3025–303.

*Percic, Marcus*, § 54 StPO in: Münchener Kommentar zur StPO 1. Auflage. München 2014.

*Perron, Walter*, Das Beweisantragsrecht des Beschuldigten – Ursache oder Symptom der Krise des deutschen Strafprozesses? ZStW 108(1)/1996, 128–154.

*Pollähne, Helmut*, Unmittelbarkeit, Unschuldvermutung und (anderweitig) Unverzichtbares – Wider den Bedeutungsverlust der Hauptverhandlung, StV 2015, 784–790.

*Poscher, Ralf*, Eingriffsschwellen im Recht der inneren Sicherheit. Ihr System im Lichte der neueren Verfassungsrechtsprechung. DV 3/2008, 345–373.

*Rimoux, Frédéric*, Kants Rechtstheorie vom Weltfrieden. Zwischen apriorischen Rechtsprinzipien und politischer Praxis (2015. Dissertation an der Eberhard Karls Universität Tübingen).

*Rogall, Klaus,* § 54 StPO in: Systematischer Kommentar zur Strafprozessordnung mit GVG und EMRK. Band I. 5. Auflage. Köln 2018.

*Roggan, Fredrik*, Die unmittelbare Nutzung geheimdienstlicher Informationen im Strafverfahren nach dem Antiterrordateigesetzt. Über die Gefahr der Kontamination der Wahrheitssuche mit Unverwertbarem, in: Rechtsstaatlicher Strafprozess und Bürgerrecht. Gedächtnisschrift für Edda Weßlau, Herzog, Felix/Schlothauer, Reinhold/Wohlers, Wolfgang, Berlin 2016, 269–291.

– Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur. NJW 2009, 257–262.

*Roggan, Fredrik/Bergmann/Nils*, Die „neue Sicherheitsarchitektur" der Bundesrepublik Deutschland. Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz. NJW 2007, 876–881.

*Rose-Stahl*, Monika, Recht der Nachrichtendienste. 2., überarbeitete Auflage. Brühl/Rheinland 2006.

*Roxin, Claus/Bernd, Schünemann*, Strafverfahrensrecht. 29. Auflage. München 2017.

*Rzepka, Dorothea*, Das Strafverfahren in den Händen der Polizei: Ist-Zustand und kriminalpolitische Visionen. KritV 1999, 312–335.

*Safferling, Christoph J. M.,* Verdeckte Ermittler im Strafverfahren – deutsche und europäische Rechtsprechung im Konflikt? NStZ 2006, 75–82.

*Schünemann, Bernd*, Die Lichtensteiner Steueraffäre als Menetekel des Rechtstaats, NStZ 2008, 305–310.

– Die Zukunft des Strafverfahrens – Abschied vom Rechtsstaat?, ZStW 119/2007, 945–958.

– Reflexionen über die Zukunft des deutschen Strafverfahrens in: Strafrecht, Unternehmensrecht, Anwaltsrecht, Festschrift für Gerd Pfeiffer, Otto Friedrich Freiherr von Gamm, Peter Raisch, Klaus Tiedemann (Hrsg.), 1988, Berlin, 461–484.

*Schuster, Frank Peter*, Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess. Berlin 2006.

*Sieber, Ulrich*, Der Paradigmenwechsel vom Strafrecht zum Sicherheitsrecht in: Tiedemann/Sieber/Burchard/Brodowski (Hrsg.), Die Verfassung moderner Strafrechtspflege. Erinnerung an Joachim Vogel, Baden-Baden 2016, 349–372.

– Ermittlungen in Sachen Liechtenstein – Fragen und erste Antworten, NJW 2008, 881–886.

*Singer, Jens*, Das Trennungsgebot – Teil 1. Politisches Schlagwort oder verfassungsrechtliche Vorgabe? Die Kriminalpolizei 2006, 85–90.

– Das Trennungsgebot – Teil 2. Politisches Schlagwort oder verfassungsrechtliche Vorgabe? Die Kriminalpolizei 2006, 112–117.

*Soiné, Michael*, Aufklärung der Organisierten Kriminalität durch den Bundesnachrichtendienst, in: Zwischen Globalisierung und Staatenzerfall – Perspektiven Organisierter Kriminalität. Gemeinsames Symposium des Landeskriminalamtes Thüringen und des Thüringer Ladesamtes für Verfassungsschutz am 27.10.2004 in Erfurt, available at https://www.thueringen.de/de/publikationen/pic/pubdownload1095.pdf, 11–22.

– Erkenntnisverwertung von Informanten und V-Personen der Nachrichtendienste in Strafverfahren, NStZ 2007, 245–253.

*Stein, Ulrich*, Die Anwesenheitspflicht des Angeklagten in der Hauptverhandlung. Versuch einer verfassungskonformen Auslegung der §§ 230, 231, 232–236 StPO, ZStW 97(2)/1985, 303–330.

*Stümper, Alfred*, Die Wandlung der Polizei in Begriff und Aufgaben. Kriminalistik 6/1980, 242–245.

*Tamm, Marina*, Rückwirkungen des gescheiterten SWIFT-Abkommens auf das Abkommen über Fluggastdaten, VuR 6/2010, 215–223.

*Trüg, Gerson and Habetha*, Jörg, Die "Liechtensteiner Steueraffäre" – Strafverfolgung durch Begehung von Straftaten? NJW 2008, 887–890.

*Theile, Hans*, Entscheidungsanmerkung zum BGH, Beschl. v. 13.6.2012 – 2 StR 112/12, ZIS 1/2013, 128–131.

*Töpfer, Eric*, Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen. Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei. Policy Paper. Deutsches Institut für Menschenrechte. Berlin 2013. [http://www.institut-fuer-menschenrechte.de/uploads/tx_commerce/Policy_Paper_21_Informationsaustausch_zwischen_Polizei_und_Nachrichtendiensten_strikt_begrenzen.pdf].

*Ventzke, Klaus-Ulrich*, Warum stellen Sie denn keinen Beweisermittlungsantrag? oder: Die revisionsrechtliche Aufklärungsrüge – ein beweisantragsrechtliches Problem, StV 2009, 655–662.

*Vogel, Benjamin*, The Core Legal Concepts and Principles Defining Criminal Law in Germany in: The Limits of Criminal Law. Anglo-German Concepts and Principles, ed. by Matthew Dyson and Benjamin Vogel, 2018, Cambridge, 39–69.

– „In camera"-Verfahren als Gewährung effektiven Rechtsschutzes? Neue Entwicklungen im europäischen Sicherheitsrecht, ZIS 1/2017, 28–38.

*Volk, Klaus*, Die Anwesenheitspflicht des Angeklagten – ein Anachronismus. In: Schöch, Heinz „u.a. (Hrsg.)", Festschrift für Reinhard Böttcher zum 70. Geburtstag, Berlin 2007, 213 – 221.

*Volkmann, Uwe*, Polizeirecht als Sozialtechnologie, NVwZ 2009, 216–222.

– Urteilsanmerkung zu BVerfG, Beschluss vom 4.4.2006, 1 BvR 518/02 (Rasterfahndung), JZ 18/2006, 918–920.

– Sicherheit und Risiko als Problem des Rechtsstaats, JZ 14/2004, 696–703.

Weißbuch 2016. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr. [https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf].

*Weigend*, Thomas and Turner Iontcheva, Jenia, The Constitutionality of Negotiated Criminal Judgments in Germany, GLJ 15/2014, 81–10.

*Weßlau*, Edda, Wahrheit und Legenden: die Debatte über den adversatorischen Strafprozess, ZIS 1/2014, 558– 564.

*Wohlers*, Wolfgang/Greco, Luís, § 96 StPO in: Systematischer Kommentar zur Strafprozessordnung. Band III. 5. Auflage. Köln 2016.

*Zoller, Manfred*, Rahmenbedingungen nachrichtendienstlicher Informationsgewinnung über das Ausland, in: Guido, Korte/Manfred, Zoller (Hrsg.), Informationsgewinnung mit nachrichtendienstlichen Mitteln: Rahmenbedingungen, Einsatzmodalitäten, Verarbeitungsaspekte. Beiträge zur Inneren Sicherheit, Fachhochschule des Bundes. Oktober 2001. 9–35 [http://www.hsbund.de/SharedDocs/Downloads/2_Zentralbereich/20_Referat_W/50_Publikationen/15_Beitraege_Innere_Sicherheit/band_16.pdf?__blob=publicationFile&v=3

*Zöller, Mark A.*, Der Rechtsrahmen der Nachrichtendienste bei der „Bekämpfung" des internationalen Terrorismus. JZ 15/16/2007, 763–771.

# List of Judgments

## With regard to Security Law

BVerfG 30, 1 = BVerfG NJW 1971, 275 ff. (strategic monitoring)

BVerfGE 65, 1 = BVerfG NJW 1984, 419 ff. (right to informational self-determination)

BVerfGE 100, 313 = BVerfG NJW 2000, 55 ff. (strategic monitoring)

BVerfGE 109, 279 = BVerfG NJW 2004, 999 ff. (residential surveillance)

BVerfGE 110, 33 = BVerfG NJW 2004, 2213 ff. (preventive wiretapping)

BVerfGE 113, 348 = BVerfG NJW 2005, 2603 ff. (precautionary wiretapping)

BVerfGE 115, 320 = BVerfG NJW 2006, 1939 ff. (preventive screening)

BVerfGE 120, 274 = BVerfG NJW 2008, 822 ff. (the use of so-called 'state trojan')

BVerfGE 120, 378 = BVerfG NJW 2008, 1505 ff. (automatic licence plate recognition)

BVerfGE 125, 260 = BVerfG NJW 2010, 833 ff. (retention of telecommunication data)

BVerfGE 130, 151 = BVerfG NJW 2012, 1419 ff. (retention of telecommunication data)

BVerfGE 133, 277 = BVerfG NJW 2013, 1499 ff. (joint counter-terrorism database)

BVerfGE 141, 220 = BVerfG NJW 2016, 1781 ff. (preventive surveillance measures)

BVerfG Decision of 18 December 2018 – 1 BvR 2795/09 (automatic licence plate recognition).

## With regard to Criminal Procedure Law

BVerfG NJW 1981, 1719 (intelligence informant)

BVerfG NJW 1983, 1043–1046 (police files)

BVerfG NJW 1996, 448 (police informant)

BVerfG NJW 2000, 1175 (*in-camera* hearing)

BVerfG NStZ-RR 2013, 379 (search warrant based on undisclosed evidence)

BGH NJW 1980, 2088 (reading out of the police minutes of the interview of a police informant)

BGH NJW 1984, 65 (hearing of police informant outside of the court by an associate judge)

BGH StV 1989, 284 (undercover agent and police informant)

BGH NStZ 2000, 265 (undercover agent and in-camera hearing)

BGH NStZ 2001, 333 (police informant)

BGH NJW 2003, 74 (hearing of undercover agent and police informant by 'video conference')

BGH NStZ 2005, 43 (hearing of undercover agent by 'video conference')

# List of Abbreviations

| | |
|---|---|
| BayPAG | Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei |
| BeckRS | Beck online Rechtsprechung |
| BfV | Bundesamt für Verfassungsschutz |
| BVerfSch-Law | Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz |
| BGH | Bundesgerichtshof |
| BGHSt | Entscheidungen des Bundesgerichtshofes in Strafsachen |
| BKA | Bundeskriminalamt |
| BND | Bundesnachrichtendienst |
| BVerfG | Bundesverfassungsgericht |
| BVerfGE | Sammlung der Entscheidungen des Bundesverfassungsgerichts |
| BVerfSchG | Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz |
| BVerwG | Bundesverwaltungsgericht |
| CCP | German Code of Criminal Procedure (StPO) |
| CR | Computer und Recht |
| DV | Die Verwaltung |
| ECHR | European Convention on Human Rights |
| ECtHR | European Court of Human Rights |
| GA | Goltdammers Archiv für Strafrecht |
| GG | Grundgesetz |
| GLJ | German Law Journal |
| GRUR | Gewerblicher Rechtsschutz und Urheberrecht |
| GSZ | Zeitschrift für das Gesamte Sicherheitsrecht |
| GVG | Gerichtsverfassungsgesetz |
| JuS | Juristische Schulung |
| JZ | JuristenZeitung |
| KritV | Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft |
| LR | Löwen-Rosenberg |
| MMR | Multimedia und Recht |
| MüKO | Münchener Kommentar zur StPO |

| | |
|---|---|
| NJOZ | Neue Juristische Online-Zeitschrift Neue Juristische Wochenschrift |
| NJW | Neue Juristische Wochenschrift |
| NStZ | Neue Zeitschrift für Strafrecht |
| NStZ-RR | Rechtsprechungsreport Strafrecht |
| NVwZ | Neue Zeitschrift für Verwaltungsrecht |
| OLG | Oberlandesgericht |
| PC | German Penal Code (StGB) |
| RiStBV | Richtlinien für das Strafverfahren und das Bußgeldverfahren |
| SK | Systematischer Kommentar zur Strafprozessordnung mit GVG und EMRK |
| StGB | Strafgesetzbuch |
| StPO | Strafprozeßordnung |
| StV | Strafverteidiger |
| VG | Verwaltungsgericht |
| VuR | Verbraucher und Recht |
| ZIS | Zeitschrift für Internationale Strafrechtsdogmatik |
| ZphF | Zeitschrift für philosophische Forschung |
| ZRP | Zeitschrift für Rechtspolitik |
| ZStW | Zeitschrift für die gesamte Strafrechtswissenschaft |

ArchiS
Architektur des Sicherheitsrechts

The present study illustrates the emergence and development of security law in Germany, focusing on concepts involving the role of the national intelligence services for purposes of crime control. It examines the underlying security polices and the constitutional limits of restructuring the intelligence, police, and criminal prosecution authorities. The resulting shifts gave rise to a complete redrawing of the boundaries between them. In order to make these shifts unambiguously clear, the authors look at the investigation thresholds in affected areas and describe how crime control can be carried out under different labels. In addition, they specifically address the problem of how intelligence information is introduced at different stages of the criminal proceedings and explain how some evidence is kept secret during the proceedings. The authors also examine the theoretical foundations in jurisprudence and in literature as well as their practical application in statutory law.

ArchiS – Architektur des Sicherheitsrechts
c/o Max-Planck-Institut für ausländisches
und internationales Strafrecht
Günterstalstr. 73
79100 Freiburg i. Br.
Germany

Tel. +49 (761) 7081-0
Fax +49 (761) 7081-294
info@mpicc.de
http://www.mpicc.de

MAX-PLANCK-GESELLSCHAFT