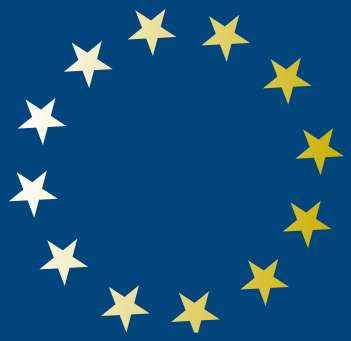
eucrim 2023 / 2

European Law Forum: Prevention • Investigation • Prosecution



## Electronic Evidence
## Preuves électroniques
## Elektronische Beweismittel

**2023 / 2** ISSUE / ÉDITION / AUSGABE

eucrim also serves as a platform for the Associations for European Criminal Law and the Protection of Financial Interests of the EU – a network of academics and practitioners. The aim of this cooperation is to develop a European criminal law which both respects civil liberties and at the same time protects European citizens and the European institutions effectively. More information about the Associations is available at: https://eucrim.eu/associations/.

# Contents

## News

### European Union



## Articles

### Electronic Evidence



### *Beyond the Focus*

# Guest Editorial

Dear Readers,

On 12 July 2023, after more than five years of, in part, very fraught negotiations, the European Parliament and the Council signed the so-called "e-evidence package". This marked the turning point in the cooperation between law enforcement authorities and service providers. Criminal offences prepared and carried out exclusively offline are a thing of the past, which is why electronic evidence is becoming increasingly important for law enforcement authorities. However, e-evidence is frequently stored in another State and, until now, cross-border access to such evidence was often very burdensome, often resulting in possibly already getting lost and causing investigations to be stopped inconclusively. The new EU internal rules will now allow national authorities to request evidence directly from service providers in other Member States or to ask that data be preserved, based on EU-wide harmonised rules and deadlines.

Driven by the singular objective of speeding up the process, however, the initial Commission proposals and partly also the Council position completely ignored the fact that criminal law across the EU is far from being fully harmonised, beginning with the question of what constitutes a (serious) crime. The drafters of the new Regulation and Directive also turned a blind eye to the fact that the rule of law and the protection of fundamental rights is not a given, not even within the EU. In my capacity as Parliament Rapporteur for the package, I have therefore done my utmost to ensure that cross-border judicial and police cooperation were adapted to today's digital reality, on the one hand, and, on the other, that fundamental rights (in particular the rights to privacy and to the protection of personal data) remain protected and procedural safeguards are ensured .

As representatives of the European Parliament, we successfully pushed for the introduction of a notification regime: When it comes to production orders for the most sensitive data categories – traffic and content data –, the State in which the service provider is addressed will (barring exceptions) have to be notified about the order. The notified authorities will then have ten days to refuse the order, based on a clear list of grounds, including concerns about media freedom and fundamental rights violations in the requesting Member State. Parliament also made sure that service providers will be able to flag concerns. Furthermore, we pushed through the introduction of a decentralised IT system, in order to ensure that orders and data are safely exchanged as well as to guarantee that service providers receive orders only from authenticated authorities.

Birgit Sippel

The years leading up to the signature of the package have been a political rollercoaster, with the European Parliament and the Council initially defending quite different positions. Personally, I would have preferred an even broader notification regime, additionally covering the ostensibly less sensitive data categories (i.e. subscriber data and IP addresses); however, this was impossible due to strong opposition from the Member States and even the conservatives in the Parliament. In the end, both sides had to compromise.

Now, the time has come for this package to be thoroughly implemented, so that it can deliver the goods we have been aiming for. The role of the European Parliament and my role as Rapporteur does not stop here. Quite the contrary! The internal rules lay only the groundwork for future international cooperation agreements. On behalf of the EU, the Commission is negotiating both a potential EU-US e-evidence agreement and a UN convention on cybercrime. As Rapporteur for the EU-US negotiations and shadow rapporteur for the UN convention, my colleagues and I will keep a very close eye on all further developments. Because one thing is clear: The protection of fundamental rights, in particular the right to privacy and the protection of one's data, is a whole new ball game beyond the EU!

**Birgit Sippel**
Member of the European Parliament

# News

## Actualités / Kurzmeldungen*

## European Union

*Reported by Thomas Wahl (TW), Cornelia Riehle (CR), Dr. Anna Pingen (AP) und Simon Haupt (SH)*

### Foundations

#### Rule of Law

##### Commission's 2023 Rule of Law Report

spot light

On 5 July 2023, the Commission published its 4th Rule of Law Report. The Rule of Law Report includes 27 country chapters and examines developments – both positive and negative – across all EU Member States in four key areas for the rule of law:

- The justice system;
- The anti-corruption framework;
- Media pluralism and freedom;
- Other institutional issues related to checks and balances.

The first Rule of Law Report was presented on 30 September 2020 (→eucrim 3/2020, 158–159); the second report on 20 July 2021 (→eucrim 3/2021, 134–135); and the third on 13 July 2022 (→eucrim 3/2022, 166–167).

The fourth report not only builds on last year's report, in which specific recommendations for all Member States were included for the first time, but it also contains a qualitative assessment of progress made by the Member States towards implementing the 2022 recommendations. The 2023 Rule of Law Report noted that almost 65% of the specific recommendations issued to Member States last year have been followed up on. However, systemic concerns remain in several Member States. Looking at said four key areas, the report highlights the following:

➤ *Justice Systems*

In order for a justice system to function and benefit all citizens and businesses, it must be independent. The perception of judicial independence by the general public has improved in 12 Member States compared to 2022, but the perception of judicial independence by companies has decreased in 13 Member States.

The recommendations of the 2022 Report were followed in a number of Member States: Legislative efforts to strengthen the independence and effectiveness of the Councils for the Judiciary were completed; they play an important role for independence in matters such as the appointment and professional career of judges and the management of the judicial system. In Slovakia, Bulgaria, Spain, Cyprus, and Poland, however, concerns regarding the Councils for the Judiciary have yet to be addressed.

Another important issue is the autonomy and independence of the prosecution service: While several Member States have initiated or continued reforms of their prosecution services, a number of identified problems remain. In Spain, for instance, no steps have been taken to strengthen the statute of the Prosecutor General and to address the separation of the Prosecutor General's term of office from that of the government.

In an effort to improve the quality and efficiency of the judiciary, positive steps have been taken in numerous Member States (e.g. by increasing the number of judges and financial resources). There has also been an improvement in digitisation and a strengthening of the right of access to a lawyer in a few Member States.

➤ *Fighting corruption*

Corruption remains a serious concern for EU citizens and businesses, with 60% of citizens believing that their government's efforts to fight corruption are not effective. The report notes that, since last year's report, various Member States have updated their national anti-corruption strategies and/or action plans or started

* Unless stated otherwise, the news items in the following sections cover the period 1 May – 15 October 2023. Have a look at the eucrim website (https://eucrim.eu), too, where all news items have been published beforehand.

the process of revising their existing strategies. Several have undertaken criminal law reforms to strengthen the fight against corruption. For example, Austria drafted legislation to extend bribery offences to candidates for public office and to include additional sanctions, such as prohibition from holding public office.

For many Member States, however, the limited resources of prosecution services remain a challenge in the fight against corruption. In order to improve criminal investigations and prosecutions, Member States need to reform and reduce the length of criminal proceedings.

While some have taken measures to address the issue of immunity for members of the government with respect to corruption offences, Poland still needs to address these issues. A few Member States introduced reforms in 2023 to address issues raised in the recommendations of 2022 regarding declarations of assets and interests by public officials (e.g. Czech Republic, Greece, Latvia, and Romania).

➤ *Media pluralism and freedom*

In order to increase the independence of media authorities or to extend their powers to other areas, new provisions have been adopted in the Czech Republic, Lithuania, and Ireland. New legislation has also been adopted in Greece, Luxembourg, and Sweden to increase the transparency of media ownership or to improve the public availability of information on media ownership.

Since the 2022 Report, several Member States have proposed or adopted legislation or established practices to improve the right of access to public information or to clarify one or more aspects of this right.

In order to address the threat of strategic lawsuits against public participation (SLAPPs) and respond to the recommendations identified in the 2022 Report, many Member States are considering introducing specific procedural safeguards and/or revising their defamation laws (e.g. Lithuania, Italy, and Slovakia).

➤ *Other institutional issues related to checks and balances*

With regard to the development of constitutional courts, the report expresses concern over developments in Poland and notes that the Commission has referred Poland to the ECJ for violations of EU law by the Constitutional Tribunal and its jurisprudence (→eucrim 1/2023, 4). Like last year, around 40% of the ECtHR's leading judgments on EU Member States from the last 10 years have not been implemented.

The report notes that civil society organisations and human rights defenders increasingly face challenges related to the narrowing of civic space and that some of the recommendations of the 2022 Report have only been partially implemented.

➤ *Perspectives*

The European Parliament and the Council are invited to continue general and country-specific debates on the basis of the Rule of Law Report. National parliaments, civil society organisations, and key stakeholders are encouraged to hold national dialogues on the rule of law with increased citizen's participation. The Commission will offer support to the Member States in addressing the challenges identified in the report and in implementing its recommendations. For the upcoming new cycle of the rule of law report, the Commission looks forward to the evaluation of the Council's Rule of Law Dialogue under the Spanish Presidency. (AP)

### Rule of law developments in Poland: May–October 2023

This news item continues the overview of rule-of-law developments in Poland (as far as they relate to European law) from 1 May to 31 October 2023. They follow up the overview in →eucrim 1/2023, 4–5.

■ 26 May 2023: The "Sejm" (lower house of the Polish legislature) adopts the law on the "State Commission for the examination of Russian interference in the internal security of Poland". After signature of the law by Polish President *Andrzej Duda* on 29 May 2023, it entered into force on 31 May 2023. The State commission is designed as an administrative committee which is part of the public administration and whose members are appointed by the Sejm. It has to examine whether high-ranking officials acted or developed "activities" to the detriment of public interests in the period 2007–2022. The mandate includes examining and deciding whether a person should be deprived of the right to hold public office in connection with the management of public funds for up to ten years. The Commission is authorised to receive classified information, conduct hearings and further investigations and amend or repeal administrative decisions, even if they were confirmed by an administrative court. The law is also nicknamed "*Lex Tusk*" since the opposition fears that the State commission will above all examine activities between 2007 and 2014 when Tusk was Polish Prime Minister; Tusk is top candidate for the opposition for the parliamentary elections on 15 October 2023.

■ 29 May 2023: The U.S. Department of Justice voices concerns over the "Lex Tusk". In a press statement, it is said that the new legislation could be misused to interfere with Poland's free and fair elections. The government of Poland is called on "to ensure this law does not preempt voters' ability to vote for candidate of their choice and that it not be invoked or abused in ways that could affect the perceived legitimacy of elections".

■ 30 May 2023: The European Commission issued a press release in which concerns are expressed with regard to the "Lex Tusk". Citizens may be deprived of their right to a fair trial.

■ 1 June 2023: Several lawyers allege that the "Lex Tusk" infringes the Polish constitution, Art. 6 ECHR and the fundamental values of the EU.

■ 5 June 2023: The ECJ delivers its judgment in Case C-204/21 – the action for failure to fulfil obligations brought by the Commission against the so-called "muzzle law" (laws amending the national rules relating to the organisation of the ordinary courts, the administrative courts and the Supreme Court of 20 December 2019 →eucrim 1/2020, 2–3 and →eucrim 1/2021, 4). The Vice-President of the CJEU recently reduced the daily penalty payment to €500,000 by an order of 21 April 2023 at Poland's request (→eucrim 1/2023, 5), because Poland had at least partially complied with the requirements of the order for giving effects to interim measures dated 14 July 2021 (→eucrim 3/2021, 135). In its final judgment, the ECJ concludes that the Polish "muzzle law" infringed Union law. It reiterates its assessment that the Disciplinary Chamber of the Supreme Court does not satisfy the requirement of independence and impartiality. The disciplinary regime and its sanctions may prevent judges from referring questions to the CJEU for a preliminary ruling and are incompatible with the guarantees of access to an independent and impartial tribunal. The transfer of responsibility for reviewing the essential requirements for effective judicial protection to one single body (i.e, the Extraordinary Review and Public Affairs Chamber of the Supreme Court) is also contrary to EU law. Lastly, the obligation of judges to submit a written declaration indicating any membership of associations, non-profit foundations or political parties disproportionately interferes with their fundamental rights (right to protection of personal data, right to respect for private life). The today's judgment terminated the effects of the penalty payment orders against Poland. However, this does not affect Poland's obligation to pay the daily penalty payments due for the past.

■ 8 June 2023: The Commission opens an infringement procedure against Poland alleging that the new law in Poland on the State Committee for the Examination of Russian influence on the internal security of Poland between 2007 and 2022 (nicknamed "Lex Tusk") violates EU law. The Commission sent a letter of formal notice to Poland and considers that the law unduly interferes with the democratic process, violates the principles of legality and of non-retroactivity of sanctions, and does not respect the right to an effective judicial remedy. In addition, the law is incompatible with EU data protection rules.

■ 23 June 2023: Journalists examined cases that have been decided by the Polish Supreme Court since 2019 and involved disputes between Polish authorities and media. They conclude that decisions taken by neo-judges, who were appointed by the conservative ruling party PiS after the judicial reforms initiated in 2018, favoured the authorities' stance.

■ 6 July 2023: The ECtHR rules that there had been several violations of fundamental rights by Poland when the country initiated preliminary inquiries against Polish district judge *Igor Tuleya* on suspicion of disciplinary misconduct. Mr Tuleya is one of the most prominent critics of the judicial reforms of the national-conservative ruling party PiS. According to the ECtHR, the criminal limb of Art. 6 para. 1 ECHR (right to a fair trial) is applicable to the immunity proceedings against Mr Tuleya. This guarantee was violated because the Disciplinary Chamber of the Supreme Court, which had examined Mr Tuleya's case, had not been an "independent and impartial tribunal established by law", as already observed in previous judgments against Poland. In addition, there had been no lawful basis for the measures against Mr Tuleya which have had a significant impact on his right to private life (Art. 8 ECHR) and could be characterised as a strategy aimed at intimidating (or even silencing) him for the views that he had expressed (Art. 10 ECHR). In conclusion, the ECtHR held that Poland was to pay Mr Tuleya €30,000 in respect of non-pecuniary damage and €6,000 in respect of costs and expenses.

■ 11 July 2023: The European Parliament (EP) approves a resolution in which the Polish authorities are urged to repeal the "Lex Tusk" (cf. supra). MEPs also submit that the Commission should pursue an expedited infringement procedure as soon as possible and apply to the CJEU for interim measures if the act remains in force. Furthermore, the EP expresses deep concerns over the recent amendments to the Polish Electoral Code that are not in line with international democratic standards.

■ 13 July 2023: In its judgment in Joined Cases C-615/20 (YP and Others) and C-671/20 (M. M.), the ECJ deals with the question as to which extent Union law allows Polish courts to disregard resolutions of the Polish Disciplinary Chamber that waived the immunity of judges and reassigned their cases to other court panels. The case concretely concerns Polish judge *Igor Tuleya* who recently won his case also before the ECtHR (→judgment of 6 July, supra). The judges in Luxembourg state that the resolutions were based on national provisions that the CJEU has held to be contrary to Union law (→cf. judgment of 5 June 2023, supra). Given the authority attached to a judgment establishing a failure to fulfil obligations on the part of a Member State and the principle of the primacy of EU law, national courts are required to disapply an act ordering, in breach of EU law, a judge's suspension from his or her duties. Consequently, Igor Tuleya must be able to continue to exercise jurisdiction in the proceedings before him and the panel, to which a case initially entrusted to Tuleya was

reassigned, must refrain from ruling on that case.

■ 27 July 2023: In an urgent opinion, the Venice Commission of the Council of Europe recommends that the Polish authorities revoke the "Law on the State Commission to Investigate Russian Influence" at their earliest convenience. The Venice Commission is particularly concerned about the overly broad scope of application of the Law and the fact that core notions are formulated in an excessively vague manner. It concludes that the Law has a negative impact on the level playing field in the context of the upcoming autumn elections.

■ 3 August 2023: Polish President *Andrzej Duda* signs off amendments to the law establishing the State Commission for the Examination of Russian influence on the internal security of Poland. The amendments come after mounting international criticism of the law passed end of May 2023 (cf. supra). Accordingly, the possibility of a ban on holding office no longer applies. Nonetheless, the Commission should be entitled to announce that persons are unsuitable for public office as there is no guarantee that they represent Poland's interests. Moreover, it would now be possible to appeal against the Commission's decisions to the Warsaw Court of Appeal. It is criticised, however, that the capital's court, which deals with most cases involving parliament, government and central authorities due to its local jurisdiction, has been almost completely filled with loyal judges as part of the ruling parties' (PiS) restructuring of the judiciary. Opponents also point out that the law is still apt to discredit Polish opposition leader Donald Tusk.

■ 30 August 2023: Polish president *Andrzej Duda* signs an amendment to the Penal Code which introduces penalties for spreading disinformation, increases penalties for espionage and bans photographing and recording objects important for the security and defence of the state. In particular, the new law (dubbed "spy act") penalises the spreading of disinformation on behalf of a foreign intelligence service with the aim of inciting interference in the society and economy of Poland with at least 8 years of imprisonment. Critics put forward that the notion of disinformation is too vast in terms of content and that this provision could open the door to investigating whether journalists or NGOs have some kind of relationship with a foreign intelligence service, and whether their actions are intended to cause some kind of serious harm.

■ 11 October 2023: Ahead of the parliamentary elections, the press reports that the ruling national conservative PiS party and its cooperating partner, Suwerenna Polska (Sovereign Poland Party), have not respected the financial rules enshrined in the Electoral Code which are to ensure that all parties have an equal level playing field in the election campaign. The Electoral Code lays down strict rules how much money can be available for parties to finance their electoral campaigns. It is maintained that politicians from the ruling party have brushed off these rules and used public money to organise *de facto* party events, advertise party election promises, and to buy equipment for voters, ranging from laptops to pots.

■ 15 October 2023: In the parliamentary elections, the national conservative party PiS ("Law and Justice") was once again the strongest force with around 35.4%, but this time it was not enough for an absolute majority. The second strongest party was the Civic Coalition (KO) with just under 31%. With a voter turnout of 74%, the highest figure since the transformation in 1989 was recorded. There are signs of a change of government, as the other parties in question have ruled out a coalition with the PiS. (TW)

### Romania: ECJ Rules on the Independence and Impartiality of Bodies in Disciplinary Proceedings against Judges

On 11 May 2023, the ECJ ruled on the compatibility of the Romanian reform of the organisation of the judiciary that rearranged the Judicial Inspectorate and led to a concentration of powers in the hands of the Chief Inspector. The case (C-817/21, *Inspecția Judiciară*) was prompted by the Bucharest Court of Appeal which has to decide on challenges against decisions by the Chief Inspector who confirmed not to take action against judges and prosecutors in disciplinary proceedings against them.

Under Romanian law, the Chief Inspector heads the Judicial Inspectorate. His decisions can be reviewed by the Deputy Chief Inspector; however, the Deputy has been appointed by the Chief Inspector, his term of office will end at the same time as that of the latter and his activities are subject to the Chief Inspector's assessment. Disciplinary action intended to punish abuses committed by the Chief Inspector can be initiated only by a member of staff whose career depends, to a large extent, on the decisions of the Chief Inspector. The referring Bucharest Court of Appeal raised the question as to whether this system is sound in terms of sufficient safeguards.

The ECJ stated that a disciplinary regime must avoid any appearance of political control of judicial activity. This was not fulfilled in the present case. The structure of the Judicial Inspectorate, in particular the fundamental dependencies of the employees, including the Deputy Chief Inspector, were such that those affected could refrain from bringing a disciplinary action against the Chief Inspector. In the end, the body in charge of disciplinary proceedings against judges must be independent and impartial, which is not given in the current Romanian system. (TW)

## Area of Freedom, Security and Justice

### 2023 EU Justice Scoreboard: Focus on Fighting Corruption

spot light

On 8 June 2023, the Commission published the 2023 EU Justice Scoreboard, which provides an overview on the effective functioning of the Member States' judicial systems by providing objective, reliable, and comparable data for the year 2022. The 11th edition of the EU Justice Scoreboard (for the 2022 Scoreboard →eucrim 2/2022, 86–87) provides data on three key elements of effective national judicial systems: efficiency, quality, and independence.

This year's edition focused on the strengthening of the economic dimension of these three aspects by including new data on efficiency in the fight against corruption. The 2023 Scoreboard also shows how judicial systems have begun to recover from the effects of the COVID-19 pandemic as regards their efficiency. The key findings can be summarised as follows:

➤ *Efficiency*

■ In general, the data from 2012 to 2021 for civil, commercial, and administrative cases show positive trends in most cases. The decrease in efficiency, quality, and independence observed in 2020 was probably due to the COVID-19 pandemic and seems to be over thanks to the different types of hybrid or online working arrangements now in place.

■ Since 2012, the duration of first-instance judicial proceedings has decreased in 12 Member States. For cases of money laundering, the average duration of first-instance proceedings is up to one year in 15 Member States, up to two years in seven Member States, and up to 3.5 years in two Member States. For corruption cases, the average duration of the trial is about one year in 12 Member States and up to about four years in the remaining five Member States for which data are available.

➤ *Quality*

■ 21 Member States require that parties pay a court fee at the beginning of the court procedure. In six Member States (Bulgaria, Estonia, Ireland, the Netherlands, Poland, and Slovenia), recipients of legal aid are not automatically exempt from paying court fees.

■ Continuing the work of the 2022 EU Justice Scoreboard, which presented a separate figure on special measures facilitating equal access to justice for persons with disabilities, the 2023 edition takes a more in-depth look by focusing on two groups: the elderly and victims of violence against women/domestic violence. The figures show that 17 Member States provide information on the rights of persons at risk of discrimination and 22 Member States provide easy physical access to court buildings. Nine Member States have taken steps to make legal aid more accessible to the elderly when needed.

■ For the first time, the Scoreboard shows a selection of specific measures for victims of violence against women/domestic violence. In 12 Member States, all safeguards are in place, but almost a quarter of Member States do not provide online access to specific information on prevention, support, and protection services for victims of domestic violence or to legal information on violence against women/domestic violence and victims' rights.

■ In 20 Member States, less than 50% of judges at the highest court level are women.

■ More Member States are providing online information about their judicial systems, and online access to court judgments has also improved slightly overall compared to 2021, particularly as regards the publication of judgments of first-instance and second-instance courts.

➤ *Judicial independence*

■ The general public's perception of judicial independence has improved in 15 Member States compared to 2016. Compared to last year, companies' perception of judicial independence has decreased in 13 Member States. For both general public and companies, the main reason for the perceived lack of independence has been interference or pressure from the government and from politicians.

➤ *New focus: Combating corruption*

The inclusion of data on anti-corruption proceedings follows the adoption of the anti-corruption package, including a proposal for a Directive on combating corruption by criminal law on 3 May 2023 (→news item of 3 August 2023). The proposal for the Directive updates and harmonises EU rules on the definition of corruption offences, covering the full range of corruption offences (i.e. bribery, misappropriation, trading in influence, abuse of function, obstruction of justice). Therefore, for the first time, the 2023 EU Justice Scoreboard provides data on specialised anti-corruption bodies, giving an overview of the nature of their powers and the rules governing their appointment. In cooperation with Member States, a new questionnaire has also been developed to collect data on the duration of court proceedings before first-instance courts in bribery cases. (AP)

## Schengen

### 2023 State of Schengen Report

On 16 May 2023, the European Commission presented the second State of Schengen Report as part of its initiative to strengthen Schengen governance (for the first report →eucrim 2/2022, 88–89) The report assesses the state of the Schengen area and acknowledges the need for continued efforts to enhance external border management, increase effectiveness of returns, and boost police cooperation.

Schengen was the most attractive and frequently visited area in the world in 2022, with 65% of the world's inter-

national tourists travelling to Europe. While additional efforts are needed to further strengthen management of the external borders, Schengen is functioning well and is overall robust as a single jurisdiction for international travel purposes. Notable achievements include the following:

- Schengen's enlargement through the recent inclusion of Croatia;
- The establishment of a new Schengen Council for strategic guidance (since March 2022);
- The introduction of tools like the European border management strategy and the operational start of the renewed Schengen Information System (SIS) in March 2023.

Key priorities outlined in the State of Schengen Report are as follows:

- Consolidating Schengen governance: Implementing a new evaluation framework with targeted country recommendations to strengthen Member States' operational capacity;
- Enhancing internal security: Operationalization of the Council recommendation on police cooperation (→eucrim 2/2022, 120) to improve intelligence sharing and common risk analysis;
- Enhancing the effectiveness of the return system: Utilizing the SIS and maximizing the possibilities outlined in the Commission Recommendation for mutual recognition of return decisions and expedited returns;
- Schengen enlargement: Urging the Council to support the inclusion of Romania and Bulgaria in Schengen to strengthen European unity;
- Phasing out lengthy internal border controls: Replacing them with alternative police cooperation measures, with border controls being reintroduced only as an exception and strictly time-limited measure of last resort;
- Improving the use of EU visa policy tools: Addressing irregular migration and security risks by monitoring the functioning of visa-free regimes, aligning third partners' visa policies with those of the EU, and abolishing risky investor citizenship and residence schemes.
- The 2023 State of Schengen Report marks the beginning of the second annual Schengen cycle. It feeds into the discussions in the Council on the policy priorities for Schengen. The Commission urges the current and incoming Council Presidencies to take these priorities forward in the Schengen Council. (AP)

### EP: Bulgaria and Romania Must Accede Schengen Area

In a resolution adopted on 12 July 2023, the European Parliament (EP) reiterated its call on the Council to approve Romania's and Bulgaria's accession to the Schengen area. MEPs regret that the Council rejected the countries' accession in a decision of 8 December 2022 (→eucrim 4/2023, 224–225). According to the resolution, this decision was without any legal justification related to accession criteria and motivated by national domestic political campaigns. In addition, the resolution stresses that the fact that Romania and Bulgaria are still outside the free-travel area burdens the businesses and populations of the two countries socially and economically. Considering the still existing border controls, the exclusion also results in damages to the environment and health.

The EP shares the Commission's position that Romania and Bulgaria have fulfilled all criteria to join the Schengen area. The current Spanish Council Presidency is called to prioritise the topic and deliberate Romania's and Bulgaria's accession by the end of 2023. (TW)

## Ukraine Conflict

### Russian Business Couple Fails before EU Court

On 6 September 2023, in Cases T-270/22 and T-272/22, the General Court of the European Union (GC) dismissed the actions brought by *Dmitry Alexandrovich Pumpyanskiy* and *Galina Evgenyevna Pumpyanskaya* against the restrictive measures adopted against them by the Council.

By decision of the Council on 9 March 2022, the two spouses were added to the list of persons to which restrictive measures apply due to their involvement in the Russian aggression against Ukraine; subsequently, their funds were frozen.

The GC found that although Dmitry Pumpyanskiy had not been directly involved in the acts of military aggression in Ukraine, he was active in economic sectors that serve as important sources of income for the government of the Russian Federation. The inclusion of Ms Pumpyanskaya was justified because of her family and business relationship considering that the holds relevant positions in her husband's companies.

Moreover, in the absence of investigative powers in third countries, the assessment of the Union authorities could be based on publicly available sources of information, reports, press articles or similar sources of information.

The restrictive measures in question are precautionary measures which undeniably lead to a restriction on the exercise of certain fundamental rights. However, according to established case law, these fundamental rights must be assessed in the light of their social function. The conditions for a restriction are met against this background in the present case. The Court found that impacts on the persons concerned are mitigated by the possibilities to use frozen funds for basic needs and to get specific authorisations permitting funds or other economic resources to be released. In addition, entering the territory of the EU is not completely excluded, for instance, in case of urgent humanitarian grounds. (TW)

### International Centre for Prosecution of Crime of Aggression against Ukraine Opened

On 3 July 2023, the newly created International Centre for the Prosecution of the Crime of Aggression against Ukraine (ICPA) officially started operation at Eurojust. Designed as a judicial hub embedded in Eurojust, the centre will support national investigations into the crime of aggression related to the war in Ukraine. Through the centre, independent prosecutors from different countries will be able to work together in the same location on a daily basis, exchange evidence in a fast and efficient manner, and agree on a common investigative and prosecution strategy. The centre will benefit from Eurojust's operational, technical, logistical, and financial structure.

A key tool for the centre will be the Core International Crimes Evidence Database (CICED) managed by Eurojust. To start, five members (Lithuania, Latvia, Estonia, Poland, and Romania) of the Joint Investigation Team on alleged core international crimes committed in Ukraine (→eucrim news of 5 May 2023) and the ICC are participating in the ICPA alongside Ukraine. In a second step, the participation of other countries and organisations, such as the EU Advisory Mission to Ukraine, will be facilitated. Furthermore, countries in possession of information or evidence relevant to the investigation of the crime of aggression against Ukraine may also request to participate. (CR)

### EU Reactions to Russian War against Ukraine: Overview July– September 2023

This news item continues the reporting on key EU reactions following the Russian invasion of Ukraine on 24 February 2022 in relation to the following aspects: the impact of the invasion on the EU's internal security policy, on criminal law, and on the protection of the EU's financial interests. The following overview covers the period from the beginning of July 2023 to the end of September 2023. For overviews of the developments from February 2022 to mid-July 2022 →eucrim 2/2022, 74–80; for the developments from the end of July 2022 to the end of October 2022 →eucrim 3/2022, 170–171; for the developments from November 2022 to December 2022 →eucrim 4/2022, 226–228; for the developments from January 2023 to June 2023 →eucrim 1/2023, 6–9.

- 5 July 2023: OLAF meets with senior management officials of the National Anti-Corruption Bureau of Ukraine (NABU), the Specialised Anti-Corruption Prosecutor's Office of Ukraine (SAPO) and the United States Agency for International Development, Office of Inspector General (USAID) to discuss the effective protection of finances. Participants exchange views on work priorities, fraud risks and main challenges that must be addressed in order to implement efficient and visible measures to fight fraud and corruption affecting the EU's and international financial assistance to Ukraine.
- 7 July 2023: The Council presidency reaches a provisional agreement with European Parliament representatives on the Act in Support of Ammunition Production (ASAP). Implementing the third track of the plan agreed by the Council on 20 March 2023 to secure the long-term increase in European ammunition production for the benefit of Ukraine and EU Member States (→eucrim 1/2023, 6–9), the regulation will mobilise €500 million from the EU budget (in current prices) as a matter of urgency in order to support the ramp-up of manufacturing capacities for the production of ground-to-ground and artillery ammunition as well as missiles.
- 12 July 2023: The plenary of the European Parliament gives green light to enter into interinstitutional negotiations on the proposal for a directive on the definition of criminal offences and penalties for the violation of restrictive Union measures (for the Commission proposal →eucrim 2/2022, 75–76). The EP backs the LIBE Committee's report adopted on 7 July 2023. It is recommended that proceeds derived from the violation of the Union's restrictive measures or instruments used to pursue the violation of restrictive measures should be subject to confiscation. If the assets are confiscated in connection with the Russian war against Ukraine or related crimes, the confiscated assets or the net proceeds from the liquidation of such assets should be used for contributions towards the reconstruction of Ukraine.
- 12 July 2023: The leaders of the G7, who convened in Vilnius (Lithuania) for the NATO summit, adopt a joint declaration of support for Ukraine in which they reaffirmed their unwavering commitment to the strategic objective of a free, independent, democratic, and sovereign Ukraine.
- 17 July 2023: The European Union issues a statement condemning Russia's decision to terminate the Black Sea Grain Initiative. The EU sees this as a way of weaponising food, with Russia further exacerbating the global food security crisis.
- 20 July 2023: The Council prolongs by six months, until 31 January 2024, the restrictive measures targeting specific sectors of the economy of the Russian Federation.
- 28 July 2023: The Council adds natural and legal person to the list of those subject to restrictive EU measures for actions that undermine or threaten the territorial integrity, sovereignty, and independence of Ukraine. The Council imposes its restrictive measures against seven Russian individuals and five entities responsible for conducting a digital information manipulation campaign, known as "RRN" (Recent Reliable News), aimed at distorting information and disseminating propaganda in support of Russia's aggression against Ukraine. In to-

tal, some 1800 individuals and entities are now subject to these restrictive EU measures.

■ 3 August 2023: In response to Belarus's involvement in Russia's war of aggression against Ukraine, the EU adopts new restrictive measures against 38 individuals and three entities from Belarus who are responsible for serious human rights violations, who contribute to the repression of civil society and democratic forces as well as against those who benefit from and support the *Lukashenko* regime. The list now includes individuals responsible for torture, propagandists, and members of the judiciary involved in the persecution of democratic opponents. It also extends to state-owned companies that have taken action against employees involved in peaceful protests, including the state-controlled conglomerate Belneftekhim. In total, the EU's restrictive measures against Belarus now cover 233 individuals and 37 entities.

■ 5 August 2023: Council Regulation (EU) 2023/1594 amending Regulation (EC) No 765/2006 enters into force. It modifies restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine. The EU imposes new targeted restrictive measures, such as an export ban on goods and technology related to aviation and space industries; prohibition of the sale, supply, transfer, or export of firearms and ammunition; expansion of export restrictions on items used by Russia in its aggression, including semiconductor devices, electronic circuits, manufacturing/testing equipment, photographic cameras, and optical components; extension of the export ban on dual-use goods and technology.

■ 7–11 August 2023: The AFCOS Latvia hosts colleagues from the Economic Security Bureau of Ukraine in order to support their capacities in protecting the financial interests of the Union. Latvian experts explain the system and measures in place in Latvia to protect the EU's financial interests. Participants also discuss improvements on the Ukraine's prevention of and fight against fraud.

■ 4 September 2023: The Commission issues a guidance note for customs authorities of the EU Member State on how to deal with blocked goods brought into the EU before any restrictions (particularly those in the context of Russia's aggression against Ukraine) applied to them. The guidance note relates to the new Art. 12e of Council Regulation (EU) No 833/2014 (introduced by the 10th sanctions package →eucrim 1/2023, 7), which regulates the conditions for the release of such blocked goods. The note provides examples for the release and exceptions.

■ 7 September 2023: The Commission issues a guidance note to help European companies identify and avoid the circumvention of sanctions. The publication was made against the backdrop of increasingly complex and opaque circumvention practices on the part of Russia in connection with the war in Ukraine. The guidelines are intended to provide EU companies with practical assistance in carrying out mandatory due diligence. The guidance note includes the successive steps to be followed when conducting strategic risk assessments, guidelines for the implementation of enhanced due diligence for companies exposed most to this risk as well as a list of warning signs (red flags) of circumvention relating to customers and business partners.

■ 22 September 2023: The Commission pays a further €1.5 billion to Ukraine. With this payment, Ukraine has so far received €13.5 billion this year under Macro-financial Assistance+.

■ 22 September 2023: The Commission publishes a list of "Common High Priority Items". These are dual-use goods that were found on the battlefield in Ukraine or critical to the development, production or use of those Russian military systems. The list aims to support due diligence and effective compliance by exporters and targeted anti-circumvention actions by customs and enforcement agencies of partner countries.

■ 28 September 2023: The Council agrees to extend the temporary protection system for Ukrainian refugees until 4 March 2025. The systems allows for immediate and collective (i.e. without the need for the examination of individual applications) protection to displaced persons who are not in a position to return to their country of origin. Currently, over 4 million Ukrainian refugees live in the EU. (AP/TW)

## Artificial Intelligence (AI)

### EP's Amendments to the AI Act

On 14 June 2023, the European Parliament adopted amendments to the legislative proposal for a regulation on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

The MEPs expanded the list of intrusive and discriminatory AI to include the following:

■ "Real-time" remote biometric identification systems in publicly accessible spaces;

■ "Post" remote biometric identification systems, with the only exception being law enforcement for the prosecution of serious crimes and only after judicial authorization;

■ Biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation);

■ AI systems aiming to detect emotions, physical features, or physiological features (e.g. facial expressions, movements, pulse frequency, or voice) when they are used in law enforcement, border management, the work-

place, and educational institutions;
- Untargeted scraping of facial images from the Internet or CCTV footage to create facial recognition databases.

AI systems intended to influence the outcome of an election or referendum or the voting behaviour of natural persons should be classified as high-risk AI systems. AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise, and structure political campaigns from an administrative and logistical point of view, are not included in this high-risk classification. By contrast, AI systems intended for biometric identification of natural persons and AI systems intended to make inferences about personal characteristics of natural persons on the basis of biometric or biometrics-based data, including emotion recognition systems (with the exception of those prohibited under this Regulation), should be classified as a high risk, according to the Parliamentarians.

The MEPs also added that, in light of the rapid pace of technological development and potential changes in the use of AI systems, the list of high-risk areas and use cases in Annex III should be subject to ongoing review by means of regular assessments.

Providers of foundation models will be required to assess and mitigate possible risks (to health, safety, fundamental rights, the environment, democracy, and the rule of law) and register their models in the EU database before their release onto the EU market. Providers of foundation models used in AI systems specifically intended to generate, with varying levels of autonomy, content such as complex text, images, audio data, and video data ("generative AI") and providers who remodel a foundation model into a generative AI system shall additionally comply with the transparency obligations outlined. They must also train, and where applicable, design and develop the foundation model in such a way as to ensure adequate safeguards against the generation of illegal content. They further have to make publicly available a sufficiently detailed summary of the use of training data protected under copyright law.

The MEPs also added the obligation for users of high-risk AI, to the extent they exercise control over the high-risk AI system, to proceed as follows:
- Implement human supervision according to the requirements laid down in this Regulation;
- Ensure that the natural persons assigned to carry out human supervision of the high-risk AI systems are competent, properly qualified and trained, and have the necessary resources in order to ensure the effective supervision of the AI system in accordance with draft Art. 14 AI Act;
- Ensure that relevant and appropriate robustness and cybersecurity measures are regularly monitored for effectiveness and are regularly adjusted or updated.

With regard to the vote in the Parliament, co-rapporteur *Brando Benifei* said: "All eyes are on us today. While Big Tech companies are sounding the alarm over their own creations, Europe has gone ahead and proposed a concrete response to the risks AI is starting to pose. We want AI's positive potential for creativity and productivity to be harnessed but we will also fight to protect our position and counter dangers to our democracies and freedoms during the negotiations with Council."

The EP's amendments to the AI Act take account of proposals made at the Conference on the Future of Europe (→eucrim 2/2022 84–85). These proposals included ensuring human oversight of AI-related processes; making full use of the potential of trustworthy AI; and using AI and translation technologies to overcome language barriers. The text will now be debated in trilogue negotiations between the EP, Council and the Commission. The AI Act is one of the priorities of the Spanish Council Presidency that started on 1 July 2023. The aim is to reach a political agreement by the end of the year. (AP)

## Legislation

### Signatories and Commission Assess Strengthened Code of Practice on Disinformation

One year after the launch of the strengthened Code of Practice on Disinformation (on 16 June 2022 →eucrim news of 22 June 2022), Commission Vice-President for Values and Transparency, *Věra Jourová*, and the Director-General of DG CNECT, *Roberto Viola*, met with the signatories of the 2022 strengthened Code of Practice on Disinformation on 5 June 2023. The agenda featured discussion on the signatories' current implementation efforts and on anticipated difficulties in the following areas:
- Improving work on fact-checking;
- Enhancing access to data for study;
- Empowering users of online platforms;
- Addressing the most recent advancements in the field of generative AI.

With regard to the new challenges, which the code should address, *Jourová* stated prior to the meeing: "[…] progress remains too slow on crucial aspects, especially when it comes to dealing with pro-Kremlin war propaganda or independent access to data. The Code should also start addressing new threats such as misuse of generative AI. As we prepare for the 2024 EU elections, I call on platforms to increase their efforts in fighting disinformation and address Russian information manipulation, and this in all Member States and languages, whether big or small."

The meeting also follows the announcement by X (formerly Twitter) of its withdrawal from the voluntary code at the end of May 2023. X is thus tak-

ing a different path from other major social networks and companies, such as Meta (the parent company of Facebook, Instagram, WhatsApp, etc.) and TikTok. Commissioner for Internal Market, *Thierry Breton*, responded to the withdrawal of X, owned *by Elon Musk*, with a post on the social network. Breton issued a reminder that, after 25 August 2023, all major platforms and search engines will have to comply with the new European Digital Services Act (DSA) requirements and that the fight against disinformation will be a legal obligation under the DSA.

On 26 September 2023, the major online platform signatories (Google, Meta, Microsoft and TikTok) delivered a second set of reports on the implementation of the Code of Practice on Disinformation. The entities provided further insight into their actions to fight disinformation, with more stable data covering a full 6-month reporting period. For the first time, new signatories of the Code (Alliance4Europe, Newtral, EFCSN and Seznam) submitted their baseline report. Given the potential of generative AI for creating and disseminating disinformation, platforms also report about their recent efforts to provide safeguards regarding new generative AI systems on their services. (AP)

## Institutions

### Council

#### New Trio Council Presidency

On 1 July 2023, the new trio Presidency of Council of the EU, composed of Spain, Belgium, and Hungary, started its 18-month term. Spain began the Presidency on 1 July 2023 (→following news item); Belgium and Hungary will hold the subsequent Presidencies in 2024.

The trio adopted a joint programme outlining common priorities. It is committed to contributing to the enhancement of the EU's resilience and strategic autonomy, for instance, by strengthening its industrial base in line with the accelerated twin green and digital transitions and by capitalizing on innovation to reinforce the EU's global competitiveness. Furthermore, the trio plans to ensure that the twin transitions are fair, just, and inclusive to enhance Europe's social dimension, especially by addressing the demographic challenges the EU is facing. Another priority is to strengthen international partnerships, multilateral cooperation, and security in all its dimensions. A further objective is to develop an ambitious and balanced trade policy, while at the same time defending EU interests more assertively based on its values -, and to strengthen the EU's capability to act in the field of security and defence.

In the area of protecting citizens and freedoms, the trio will focus on reinforcing the rule of law; on reforming the European Asylum System, the Pact on Migration and Asylum, and the external dimension of migration; and on ensuring the functioning and resilience of the Schengen area. Judicial cooperation and the digitalisation of justice are also priorities, along with streamlining the EU's crisis management structures, implementing the EU's cybersecurity strategy, and achieving greater strategic autonomy in digital technologies.

Looking at criminal matters, the trio will step up efforts to counter serious cross-border organised crime, terrorism, and violent extremism, including the fight against smuggling of/trafficking in human beings, arms smuggling, and funding for extremist purposes. The prevention of terrorism and providing aid to victims of terrorism are also high on the agenda. A special focus will be placed on combating child sexual abuse, violence against women and gender-based violence, hate speech and hate crimes, racism, antisemitism, xenophobia, and other forms of intolerance. (CR)

#### Spain Takes Over Council Presidency

On 1 July 2023, Spain took over the Presidency of the Council of the EU. Spain is the first Member State in the current new trio presidency composed of Spain, Belgium, and Hungary, with the latter two holding the presidencies in 2024 (→previous news item). "Europe, closer" is the motto of the Spanish Presidency`s programme that sets out four priorities for its six-month term:

- Reindustrialising the EU and guaranteeing its open strategic autonomy;
- Advancing in the green transition;
- Promoting greater social and economic justice;
- Strengthening European unity.

Overall, the Spanish Presidency will carry on the EU's support for Ukraine and promote in-depth and improved institutional decision-making processes alongside the enlargement of the EU.

In the area of freedom, security and justice, the Spain will continue to promote, *inter alia*, the digitalization of the justice system, the consolidation of the rule of law, and the EU's accession to the European Convention on Human Rights. Priorities in the field of home affairs will be given to the Pact on Migration and Asylum, the external dimension of migration, designing a migration policy, and the functioning of the Schengen area with a view to allowing Romania and Bulgaria to fully participate in the Schengen area (→eucrim news of 26 July 2023).

Regarding criminal matters, the Spanish Council Presidency is committed to continuing the negotiations with the European Parliament on the proposals for environmental protection, confiscation and asset recovery, combating violence against women and domestic violence as well as the prevention of and fight against trafficking in human beings. It will also facilitate the negotiations on the pro-

posal for a Directive on the transfer of criminal proceedings (→eucrim news of 11 July 2023). Furthermore, the Presidency intends to advance negotiations on the proposals for a Regulation against child sexual abuse online (→eucrim 2/2022, 91–92) and for a Directive on combating corruption. The role of Eurojust in the fight against cross-border organized crime and the role of the European Public Prosecutor's Office (EPPO) in the fight against fraud to the EU's financial interests will also be further promoted. Additional priorities in the field of criminal law will be: preventing and combating terrorism and violent radicalization, including protection of the victims of terrorism and raising social awareness about the violence they experience, the fight against terrorist financing, the use of new technologies, and the threat posed by returning foreign terrorist fighters. (CR)

### Results of the Swedish Council Presidency

On 30 June 2023, the term of the Swedish Presidency of the Council of the EU (→eucrim news of 3 February 2023) ended with the handing over of the Presidency to Spain as of 1 July 2023. A scoreboard with all 321 decisions and agreements on EU laws and other texts that were finalised by the Swedish Presidency can be found here.

In the area of Justice and Home Affairs, the Swedish Presidency maintained a continuous dialogue in the JHA Council on the consequences of Russia's aggression against Ukraine for internal security (→eucrim news of 12 July 2023). Sweden also undertook efforts to fight organised crime in several areas. For instance, final agreements could be reached on the following:

- The Regulation establishing a collaboration platform to support the functioning of joint investigation teams (→eucrim news of 29 January 2022);
- The Directive on the exchange of information between the law enforcement authorities of Member States (IED) (→eucrim spotlight of 12 July 2023);
- The e-evidence Regulation.
- Negotiations have begun on the Directive on the transfer of criminal proceedings (→eucrim news of 11 July 2023), and general approaches have been reached on the following directives:
- The Directive on asset recovery and confiscation (→eucrim 2/2022, 76);
- The Directive on trafficking in human beings;
- The Directive on combating violence against women and domestic violence.

Political agreement with the European Parliament was achieved in the following matters:

- The Directive on the stronger mandate of the EU Drugs Agency;
- Law enforcement agencies' access to bank account registers;
- The digitalisation of judicial cooperation.

In addition, conclusions on an action plan for future European forensic cooperation and on measures to combat illicit trafficking in cultural goods were able to be adopted. The JHA Council has also advanced the negotiations on the legal instrument to combat child sexual abuse online (→eucrim 2/2022, 91–92). Lastly, a high-level group was tasked with addressing operational challenges as regards law enforcement access to digital information. (CR)

## OLAF

### AG: Plausibility Test for OLAF Report Required

On 13 July 2023, Advocate General (AG) *Laila Medina* provided her opinion in an appeal case in which compensation due to false accusations from the part of OLAF is claimed (Case C-363/22 P).

The initial case dates back to 2003 when OLAF reported possible criminal liability of Planistat Europe and its director *Hervé-Patrick Charlot*. After having opened an external investigation against Planistat, OLAF forwarded information to the French judicial authorities in March 2003 giving rise to offences of misappropriation of EU funds and complicity in breach of trust. However, French courts subsequently dismissed criminal proceedings against the persons under investigations. Planistat and its Director then sought compensation from the Commission for non-contractual liability and put forward several arguments in favour of a breach of obligations from the part of the Commission and OLAF during the proceedings. On 6 April 2022, the General Court (GC) dismissed the action by finding that there was no unlawful or defamatory behaviour on the part of OLAF or the Commission. The persons concerned appealed against this decision.

The AG examined the necessary scope of judicial review that has to be carried out by the GC. She concluded that the GC's judgment should partly be put aside. First, the GC had to carry out a "plausibility test". Since the duty of care as part of the principle of good administration requires OLAF to exercise caution and care as to whether any information/material it possesses is sufficient to justify reporting the matter to the national judicial authorities, the GC must verify whether the information forwarded *appeared plausible*. To that end, it was for the GC to establish whether OLAF had sufficiently precise material evidence showing that there were plausible reasons to consider that the information forwarded concerned matters liable to be characterised as criminal. In the judgement under appeal, the GC however relied on the assessment by OLAF and repeated the procedure, but failed to show that OLAF was *itself* entitled to consider that the matters in ques-

tion were liable to be characterised as criminal.

Second, the AG pointed out that it was for the GC to duly consider arguments of false accusations made by OLAF and the Commission. The GC should have examined those arguments in the light of the right to private life and the right to good administration enshrined respectively in Art. 7 and Art. 41 of the Charter. The AG emphasised, however, that the argument of false accusation can only succeed if the appellants demonstrate, at first instance, that OLAF *intentionally* forwarded false information to the national authorities; inadvertence or negligence is not sufficient.

Regarding the appellants' argument that the Commission acted wrongfully by lodging a complaint against the dismissal of the criminal proceedings before the French courts and by applying to become a civil party in the French criminal proceedings because the Commission should have first verified the truth of the information contained in the complaint, the AG sees no error in the GC's rejection of this argument. The AG argues, *inter alia*, that the Commission cannot be required to verify information forwarded by OLAF, because this would encroach on OLAF's powers and independence. (TW)

### General Court Ruled on Liability in Case of Press Leaks of OLAF Reports

In its judgment of 28 June 2023, the General Court (GC) ruled on the compensation of damage caused by press leaks of OLAF reports. In the case at issue (Case T-752/20), the International Management Group (IMG) seeks compensation for the material and non-material damage which it claims to have suffered as a result of the unlawfulness of the conduct of the European Commission and OLAF following an OLAF report concerning IMG. IMG concluded several agreements with the European Commission to implement EU funding but the OLAF report found that it might not have been entitled to do so within the meaning of the EU financial regulations. Shortly after the report was sent to the competent national authorities and the Commission, news magazines reported on the contents of the report. The Commission's investigations have failed to identify the source of the press leaks.

IMG argued that the Commission and OLAF breached their obligations to ensure confidentiality of the OLAF reports and claimed the Commission's non-contractual liability. In essence, the GC had to give a verdict on the scope of the duty of diligence following the disclosure of a document to the press.

The GC dismissed the action. It argued that it cannot be deduced from the obligation of confidentiality and professional secrecy (in particular established by Arts. 11(3), 10(1) and 10(3) of Regulation 883/2013) that the Commission would have had the duty to publicly condemn a leak and to put an end to the dissemination of false information caused by that leak by means of the publication of a press release. The failure of confidentiality lies in the leak and not in the Commission's omission. However, the leak cannot be imputed to the Commission.

The GC adds that, even assuming that the Commission was under a legal obligation to act by virtue of its duty to act diligently, it cannot be held that the breach of that duty, alleged by the applicant, constitutes a sufficiently serious breach of a rule of law intended to confer rights on individuals. In sum, the conditions to trigger the Union's non-contractual liability according to Art. 340 TFEU were not fulfilled. (TW)

### OLAF Annual Report 2022

In 2022, OLAF defended over €600 million against fraud and other irregularities harming the EU budget. In addition, OLAF's work in 2022 was marked by providing a risk framework for the Recovery and Resilience Facility, offering assistance to Ukraine authorities to ensure protection of EU funding following Russian's aggression in Ukraine, and addressing the "Qatargate" scandal that rocked the European Parliament. On 6 June 2023, OLAF presented the key achievements of its work in its annual report for 2022. For the first time, the report was made available in an interactive virtual format. The key figures regarding OLAF's investigative performance in 2022 are as follows (for activity reports of previous years, →eucrim 2/2022, 94 and eucrim 2/2021, 80–81 with further references):

- OLAF concluded 256 investigations and issued 275 recommendations to the relevant national and EU authorities;
- OLAF recommended the recovery of nearly €427 million to the EU budget, and prevented the undue spending of nearly €198 million;
- OLAF opened 192 new investigations, after having carried out 1,017 preliminary analyses;
- OLAF reported 71 cases with possible criminal offences to the European Public Prosecutor's Office (EPPO);
- OLAF closed 38 investigations into fraudulent or irregular behaviour by staff and members of the EU's institutions.

The report confirms trends that have been observed over previous years: OLAF's investigations mostly dealt with collusion, manipulation of procurement procedures, conflicts of interests, inflated invoices, evasion of customs duties, smuggling and counterfeiting. There is an increase in fraud taking place digitally and affecting multiple jurisdictions. This has posed new challenges for OLAF, i.e., the access to and processing of data becomes more and more relevant as does the work over boundaries in order to get a complete picture of the fraudulent activities.

As in previous years, the report highlights several cases which dem-

onstrate the broad scope of OLAF's mission, including fraud in an archeological site, subsidy fraud, breach of fellowship obligations, breach of procurement rules by a public administration, and fictitious employment. In addition, the report provides information on joint customs operations and examples of successful cooperation between OLAF and its partners (authorities in EU Member States and third countries).

When presenting the report, OLAF Director-General *Ville Itälä* said that OLAF protects both the EU budget and EU citizens. He emphasised that OLAF ensured that the EU taxpayers' money has been available for infrastructure and digitalisation and that EU citizens have been protected from adulterated honey, counterfeit cigarettes or dangerous alcoholic drinks. 531 million illicitly traded cigarettes and 14.7 million litres of illicit wine, beer and spirits were seized with the support of OLAF in 2022. (TW)

### OLAF Strengthens Cooperation with World Bank

OLAF further strengthened its cooperation with the World Bank. On 13 June 2023, OLAF Director-General *Ville Itälä* and GIA Vice President and Auditor General *Anke D'Angelo* signed an administrative cooperation arrangement in Brussels. GIA – the Group Internal Audit Vice Presidency of the World Bank Group – monitors and assesses whether the risk management, control, and governance processes of the World Bank Group are adequately designed and operating effectively. GIA is an important pillar of the World Bank Group's

oversight and accountability architecture. The administrative cooperation arrangement improves cooperation between the two bodies, in particular as regards oversight, exchange of information and joint activities related to the detection and prevention of irregularities and other illegal activities affecting the EU's and the World Bank Group's financial interests. The arrangement supplements an administrative cooperation agreement in place with the World Bank's Integrity Vice Presidency (INT), which was concluded in 2014. (TW)

### OLAF Gets Access to Trade and Companies Information in France

On 5 June 2023, OLAF signed an agreement which enables the Office to get direct access to legal and financial information held by clerks in France. The cooperation agreement was concluded with the French National Council of Commercial Court Clerks (*Conseil National des Greffiers des Tribunaux de Commerce,* CNGTC) and GIE Infogreffe. The latter is a service that provides the distribution of legal and economic information on business companies on behalf of all of the Registries of all French commercial courts. OLAF is now able to have (real-time) access to information from the trade and companies register and to other legal registers. Such agreements are important for OLAF's work since gathering of data for operational analyses is becoming more efficient and faster. (TW)

### OLAF Operational Work: June–September 2023

This news item summarises OLAF's operational work from June to September 2023 in chronological order. It follows the overview in eucrim 1/2023, 16–17.

■ 15 June 2023: OLAF informs of the results of operation LUDUS III, which was led by Europol and targeted fake and illicit toys that were to be sold in the European Union. In the period between October 2022 and February 2023, authorities in 20 Member States carried out over 6000 inspections and seized 19 million toys with a value of around €79 million. OLAF supported operations by coordinating targeted enforcement actions and carrying out data analysis. In addition, OLAF assisted two raids of wholesale shops in Poland.

■ 17 July 2023: Following on-the-spot checks by OLAF investigators and Greek law enforcement authorities, over 15 tonnes of illicit refrigerant gases are seized. OLAF provided intelligence on the suspicious economic operators that were checked, helped coordinate activities, and ensured cooperation with the industry operators affected by the imitated gases. Illicit trade in refrigerant gases, the use of which is restricted in the EU, is a repeating issue in OLAF's work. In March 2023, the Office obtained the Montreal Protocol Award for Customs and Enforcement Officers for its work in this domain.

■ 24 July 2023: With the support of OLAF, Romanian law enforcement authorities stop 353 litres of insecticide valued at around €100,000 in the Tulcea County (Romania). Two persons suspected of trafficking in toxic products and violations of trademark regulations are arrested. OLAF provided intelligence and coordinated the activities of the Romanian authorities.

■ 23 August 2023: Together with the European Public Prosecutor's Office (EPPO) in Bulgaria, OLAF has conducted investigations into possible irregularities in an EU-funded project for the modernisation of local railway infrastructure in Bulgaria. While the EPPO focuses on possible criminal offences, such as the misuse of EU funds, OLAF investigated the financial damage caused by the alleged irregularities, notably during the procurement procedure and project implementation. It was found that project partners either lacked the technical capacities to implement the project or had misrepresented their financial capacities. OLAF addressed a recommendation to CINEA (the European Climate, Environment and Infrastructure Executive Agency) to

recover over €38 million. The EPPO's criminal investigations are ongoing.

- 19 September 2023: On the basis of an OLAF recommendation, the Debrecen District Public Prosecution Service (Hungary) indicts two trustees of two Hungarian foundations for having falsely accounted the use of budget funds. OLAF investigations in irregularities found that the two foundations have not properly used EU and national funds that were allocated for the organisation of leisure/recreational programmes in Hungarian municipalities. (TW)

## European Public Prosecutor's Office

### AG Argues for Limited Judicial Review in EPPO's Cross-Border Investigations

**spot light**

On 22 June 2023, Advocate General (AG) *Tamara Ćapeta* delivered her opinion in Case C-281/22 (G.K. and Others) – the first case before the CJEU regarding the interpretation of the EPPO Regulation 2017/1939 (→eucrim 2/2022, 96). The case deals with cross-border cooperation between the handling European Delegated Prosecutor (EDP) in Germany who conducts the principal investigation and the assisting EDP in Austria who is requested to carry out searches and seizures against suspects under investigation in accordance with Arts. 31 and 32 of the EPPO Regulation.

The questions for a preliminary ruling were put forward by the Higher Regional Court of Vienna, Austria (*Oberlandesgericht Wien*), which has to decide on appeals by the suspects; they argued that the search and seizure measure was unnecessary and disproportional as well as contrary to fundamental rights. Given that judicial authorisation for the investigative measures is needed under Austrian law but the EPPO Regulation is rather silent on the scope of review, the Vienna Court asked:

- Whether the Austrian judge must examine all material aspects, such as criminal liability, suspicion of a criminal offence, necessity and proportionality;
- To which extent prior judicial authorisation in the Member State of the handling EDP plays a role;
- To which extent a judicial review must take place in the Member State of the assisting EDP.

AG *Ćapeta* first states that the answer to the questions is not easy and that the ECJ will have different interpretative options. Accordingly, application of the standard interpretative methods (text, context, objective and legal history) does not lead to an unequivocal result. The AG points out that the judges in Luxembourg must finally choose between two options: Option one entails a full review in the Member State of the assisting EDP – this was advcocated by the Austrian and German governments relying on the wording of Art. 31(3) EPPO Regulation. Option two would favour a division of tasks within the judicial authorisation, i.e., the court in the assisting EDP's Member State only makes a review of the formal and procedural aspects relating to the execution of the measure. This option was backed by the EPPO, the Commission, and the French, Romanian and Netherlands Governments.

AG *Ćapeta* supports option two, emphasising above all the intention of the EPPO Regulation to provide an efficient mechanism in the fight against crimes damaging the EU's financial interests, including cross-border investigations. Full judicial review in the Member State of the assisting EDP would result in the EPPO cross-border investigations being less efficient than intended.

In addition, the AG is of the opinion that the solution, which results in the judicial review in the assisting Member State being limited to procedural aspects related to the execution of the investigative measure also sufficiently safeguards fundamental rights of suspects and accused persons in cross-border investigations. In this context, the AG specifically points out the system of the EPPO Regulation that contains various safeguards guaranteeing the protection of fundamental rights, such as a concrete list of rights of suspects and accused persons in EPPO procedures, and the obligation of Member States to provide judicial remedies against EPPO's procedural acts.

In light of these considerations, the AG advises the ECJ to interpret Arts. 31(3) and 32 EPPO Regulation with regard to cross-border investigations as follows:

- The court approving a measure to be carried out in the Member State of the assisting EDP may assess only the aspects related to the execution of an investigative measure;
- The court in the Member State of the assisting EDP must accept the assessment by the handling EDP that the measure is justified, whether or not the latter is approved by prior judicial authorisation of the court in the Member State of the handling EDP.

The AG's opinion differs from the European defence lawyers' view who argued for full review powers of the court in the assisting Member States (similar to the arguments put forward by the Austrian and German Governments in the proceedings before the ECJ) and expressly objected to a preponderance of effectiveness considerations (→eucrim 1/2023, 17).

For a critical analysis of the AG' Opinion →eucrim article "Efficiency contra legem?" by H. H. Herrnfeld (in this issue, p. 229). For the request for a preliminary ruling by the Higher Regional Court of Vienna →A. Venegoni, "The EPPO Faces its First Important Test: A Brief Analysis of the Request for a Preliminary Ruling in G. K. and Others", eucrim 4/2022, 282–285. (TW)

### Launch of EPPO Academy

On 27 September 2023, European Chief Prosecutor, *Laura Codruța Kövesi*, and the General Commander of the Guardia di Finanza, *Andrea De Gennaro*, signed a working arrangement for a specific training programme for investigators. The signature marks the launch of the "EPPO Academy". Within the framework of the Italian Economic-Financial Police School, law enforcement officers from the 22 participating Member States will have the opportunity to receive specific training on PIF cases and EPPO's investigations in 2024. The training programme aims at overcoming the current lack of experience in investigations into financial and economic crimes in general, and crimes affecting the EU budget in particular. (TW)

### Working Arrangement with Danish Ministry of Justice

In August 2023, the European Chief Prosecutor, *Laura Codruța Kövesi*, and the Minister of Justice of the Kingdom of Denmark, *Peter Hummelgaard*, signed a working arrangement on the cooperation between the EPPO and the Ministry of Justice of the Kingdom of Denmark. The main aim of the arrangement is to establish facilitated cooperation in judicial criminal matters as to the application of the European Arrest Warrant, the gathering of evidence under the relevant European MLA instruments and other forms of judicial cooperation.

Both parties assure that they will support each other in the implementation of their data protection obligations. In addition, the arrangement provides for the exchange of strategic information, the secondment of Danish liaison officers to the EPPO, and EPPO contact points in Denmark. Eventually, the Parties will organise high-level and technical meetings at both operational and administrative levels and cooperate in organising trainings in matters of common interest.

The arrangement with the Danish Ministry of Justice is the second one with a judicial authority in a non-participating EU Member State. In April 2021, a similar working arrangement was concluded with the Prosecutor-General of Hungary (→eucrim 1/2021, 14). (TW)

### Arrangement with Ukrainian Anti-Corruption Authority

On 3 July 2023, the EPPO and National Anti-Corruption Bureau of Ukraine (NABU) concluded a working arrangement which aims to foster cooperation particularly in corruption cases affecting the EU's financial interests.

Regarding operational cooperation, the parties will provide mutual legal assistance to each other and share information available in their respective databases. Information can be exchanged either spontaneously or on motivated request and direct access to the databases is foreseen. The parties agree that MLA requests can be transmitted directly to each other in accordance with the CoE 1957 MLA convention and its protocols. The NABU may also take part in joint investigation teams established by the EPPO and the judicial authorities of Ukraine.

The parties may exchange strategic information and invite each other to training events. In addition, both high-level meetings and technical meetings may be organised. The EPPO also affirms that it will provide technical support to the NABU. Lastly, the arrangement includes several data protection rules.

The arrangement with the NABU is the second one with Ukrainian authorities. In March 2022, the EPPO signed a working arrangement with the Ukrainian Prosecutor General's Office (→eucrim 1/2022, 16). (TW)

### Arrangement with Special Prosecution Service in Albania

On 29 June 2023, the EPPO concluded a working arrangement with the Special Anti-Corruption and Organised Crime Structure of the Republic of Albania (SPAK). SPAK is a specialised prosecution service independent from the General Prosecutor's Office of Albania. With the latter, the EPPO signed a working arrangement in July 2022.

The arrangement covers operational and strategic cooperation as well as institutional matters and provides several rules on data protection. The parties affirm that they will closely cooperate on the basis of the relevant CoE treaties regarding the gathering of evidence, the freezing of assets, the establishment of joint investigation teams, and extradition.

SPAK may second a liaison officer to EPPO's headquarters in Luxembourg. The parties also agreed to organise both high-level meetings between the European Chief Prosecutor and SPAK's Chief Special Prosecutor and technical meetings. The parties may also cooperate in organising common training events. (TW)

### EPPO's Operational Activities: May–September 2023

The following provides an overview of EPPO's main operational activities from 1 May to 30 September 2023. It continues the periodic reports of the last issues (for the previous overview →eucrim 1/2023, 19–22). The overview is in reverse chronological order.

- 26 September 2023: On behalf of the EPPO in Madrid (Spain), law enforcement authorities conduct searches in several provinces in Spain concerning an estimated €17 million VAT fraud case. The case involves an organised criminal network, which committed intr-community VAT fraud involving the sale of luxury cars. The network also involved companies in Portugal and Germany. The raid resulted in 49 arrests, the seizure of luxury cars and cash, and the seizure of an extensive amounts of documents.
- 26 September 2023: Six people are arrested and six locations searched in

Bulgaria following an EPPO investigation into agricultural fraud committed by an organized crime group. Suspects are supposed to have provided false information on behalf of other persons to the competent authorities in order to obtain agricultural funding. Seemingly, two public officials from the State Fund Agriculture and the District may have served as members of the organised criminal group.

■ 25/26 September 2023: Spanish police arrests 23 people believed to belong to an organised criminal group that illegally obtained money from EU agricultural funds. Without knowledge of the real land owners, the suspects simulated property rights or resorted to false lease contracts in order to meet the criteria from the Common Agricultural Policy fund. The damage to the EU budges is around €3 million.

■ 19 September 2023: The EPPO in n Cluj-Napoca (Romania) has house searches carried out in Sibiu County (Romania) against employees of Lucian Blaga University of Sibiu. The investigations concern fraud in Erasmus funds. Allegedly, contracts with Asian students were forged in order to receive EU funding from the Erasmus+ Programme. The damage amounts to around €1 million.

■ 15 September 2023: The Guardia di Finanza seizes €80,000 in the framework of an EPPO investigation into agricultural funding fraud. The defendants are accused of having deceived the authorities as to the ownership of land in order to receive EU agricultural subsidies. €80,000 were unduly obtained between 2013 and 2022.

■ 1 September 2023: The EPPO in Riga (Latvia) files an indictment against two individuals and one company for procurement fraud involving EU funds of €95,000. They are accused of having unlawfully consipired in a procurement procedure for a project for the reconstruction of drainage systems, co-funded by the EU.

■ 22 August 2023: Upon request by the EPPO in Rome (Italy), the Guardia di Finanza seizes €1 million in an investigation against an NGO in Sardinia. The NGO allegedly misused EU funds made availabe for training and information activities to develop environmentally sustainable tourism in the Mediterranean.

■ 11 August 2023: The EPPO in Sofia (Bulgaria) has several locations in Bulgaria searched. Under investigation is fraud in connection with the modernisation of the Bulgarian railway, involving a total of over €241 million. Several inidviduals and companies are suspected of having misused EU funds and committed money laundering. Investigations revealed that seemingly several fictitious money transfers to a chain of hollow companies were made and criminals withdrew cash amounting to €2.5 billion.

■ 3 August 2023: The EPPO in Romania has 17 searches in homes of public officials and in public institutions carried out in an investigation into a €1.6 million fraud from employment funds. The public officials are alleged of having supported an organised crime group that illegally received EU and national funds for unemployed people training. The organised criminal group is also under investigation by the EPPO. Searches in companies of this group were carried out on 15 February 2023 (→eucrim 1/2023, 21).

■ 27 July 2023: After law enforcement authorities had raided several locations throughout Germany on 12 May 2023, the EPPO in Berlin (Germany) files an indictment against eight suspects who have allegedly been involved in a large-scale VAT fraud. The organised crime scheme evaded VAT by having established a complex network of shell companies and straw men with regard to the trade in luxury cars and medical face masks. The damage is estimated at €80 million. It is suspected that the organised crime group had a turnover of hundreds of millions of euro. Criminal activities included missing trader VAT fraud, forgery of documents, false notarisation, and money laundering. EPPO investigations also entailed law enforcement measures in Austria, Croatia, Czechia, France, and Poland.

■ 19 July 2023: The EPPO in Bratislava (Slovakia) has six persons arrested who are involved in a €3.2 million fraud. Under investigation are managers and staff of a company which received EU funds for innovative production processes for cider and beer. Investigations revealed several criminal activities, such as manipulated procurement, issuance of untrue invoices and credit fraud. Investigations also target two public officials from the Slovak Innovation and Energy Agency for corruption.

■ 19 July 2023: Upon request by the EPPO in Bologna (Italy), a freezing order of €2 million is executed against a textile trading company in Prato. The company used false purchase invoices in order to conceal that textiles were actually imported directly from China, thus avoiding VAT and customs duties. In addition to the freezing order, fabric with a value of €4.5 million was seized.

■ 18/19 July 2023: Several searches are carried out in locations in Bulgaria on the basis of investigations by the EPPO in Paris and Sofia against an organised crime group. The group is alleged of having traded luxury cars without paying VAT. Proceeds of the frauds were laundered. Bulgarian law enforcement authorities seize €73,000 in cash as well as gold and foreign currencies.

■ 17 July 2023: An investigation led by the EPPO in Valletta (Malta) leads to the arrest of eight suspects and the seizure of luxury cars and cash at several locations in Malta. The investigations target a scheme of evasion of taxes and customs duties on the importation of clothing and other goods from China. Suspects underdeclared the value and the weights of the

goods. It is assumed that they collaborated with customs officials, thus the investigations also involve corruption offences next to customs fraud and money laundering.

■ 13 July 2023: As part of an investigation into aggravated fraud involving agricultural subsidies for young farmers, led by the EPPO in Bologna (Italy), a freezing order of €153,000 is executed in the province of Parma. It is assumed that the lega respresentative of an agricultural company falsely claimed to be a young farmer managing a new farm, in order to obtain subsidies from the European Agricultural Fund for Rural Development (EAFRD).

■ 11 July 2023: In an investigation regarding subsidy fraud and money laundering, conducted by the EPPO in Iași (Romania), a Romanian company is searched and several suspects are questioned. The company, which paints icons for restaurants and the hospitality sector, obtained EU funding for a project to purchase equipment to support artistic creation. However, the equipment was bought in China at a low price through a bogus company that charged the beneficiary of the funds ten times the original price. The authority managing the funds was misled by false invoices and forged documents. It is believed that the illicit profit amounts to €80,000.

■ 5 July 2023: On behalf of the EPPO in Rome (Italy), bank accounts of a company are seized in order to secure the recovery of damage to the EU budget that amounts to €570,000. Investigations by the EPPO and the Italian agricultural payments agency AGEA found that the company was not entitled to being reimbursement for the supply of dairy products to primary schools since it has not paid the suppliers. The project was financed by the European Agricultural Guarantee Fund (EAGF) to develop healthy eating habits at schools.

■ 4 July 2023: The Guardia di Finanza seizes 13 properties, 4 plots of land and €400 000 of money in several cities in Italy in connection with an investigation conducted by the EPPO in Turin. A company is suspected of having illegally obtained around €3 million in EU and national funds to present their machines for food packaging at trade fairs abroad by providing false financial statements and misleading officials as to its financial situation.

■ 30 June 2023: The EPPO in Palermo (Italy) has a preventive seizure order carried out against a farm suspected of agricultural funding fraud. EPPO investigations found evidence that an agricultural company located in the municipality of Caronia deceived the Italian agricultural payments agency AGEA as to the possession of numerous agricultural land parcels. The suspect submitted false lease contracts, bearing the signatures of unsuspecting owners, who were unaware of the fraudulent scheme. The damage to the budget amounts to around €530,000.

■ 30 June 2023: The EPPO in Bologna (Italy) closes an investigation into fraud involving the illegal trade in fabrics from China. The EPPO has €4 million confiscated and the main offender accepted a plea bargain. Investigations revealed that the true origin and movements of the imported fabrics were disguised, *inter alia* by using shell companies in Germany and Hungary. In doing so, the fraudster did not pay customs duties and VAT, but sold the goods with profits in Italy.

■ 28 June 2023: Romanian law enforcement authorities arrest three suspects and seize real estate of up to €8.5 million with regard to an investigation by the EPPO in Iași (Romania). The suspects unduly obtained EU funds (approximately €4 million) for the purpose of purchasing medical and IT equipment and software licenses. In order to raise the private contribution for the equipment, the suspects inflated the prices and simulated the circulation of invoices between companies under their control. Illicit profits were partly used on leisure activities, vacancies and the maintenance of a power-yacht.

■ 16 June 2023: The EPPO in Zlín (Czechia) charges three persons who worked for the National History Museum in Olomouc with subsidy and procurement fraud. The defendants claimed funds from the EU's Programme for Research, Development and Education, but evidence shows that several members of the museum team have not carried out any activities for the funded project. Furthermore, two defendants are accused of having illicitly favoured a specific supplier during the public procurement procedure for a public project contract. The damage to the EU budget is estimated at around €560,000.

■ 16 June 2023: The EPPO in Prague (Czechia) charges 13 individuals and three companies with subsidy fraud involving the acquisition of manufacturing machinery, with estimated damages of up to €3 million. The suspects are alleged to have unduly obtained more than €2.9 million in EU funding. Instead of buying new and innovative machinery for welding and cutting metals, supported by the EU's Operational Programme Enterprise and Innovation for Competitiveness, the manufacturer purchased cheap and old machineries and colluded with suppliers to issue papers that justify the payment of the EU funds.

■ 15 June 2023: The EPPO in Liberec (Czechia) charges three individuals and one company with subsidy fraud involving a disinfectant production facility. According to the investigations, one of the accused and his two accomplices artificially inflated the prices of machines, thus fraudulently obtaining €800,000 from the European Regional Development Fund. The Czech police seized the production facility as well as assets and real estate of the defendants in order to secure the recovery of the damages to the EU budget.

■ 14/19 June 2023: 27 premises are searched, cars and luxury goods seized and four persons arrested in France and in the Netherlands as part of an EPPO investigation into VAT evasion involving cars. According to EPPO's investigations, new cars were sold as second-hand which allowed the fraudsters to pay a reduced VAT rate (in case of sales of second-hand vehicles, car companies only have to pay VAT on the difference between the price paid for the vehicle and the price for which it is sold, and not for the net value of the car). It is estimated that €13 million was lost in unpaid VAT in France and €6 million in the Netherlands.

■ 14 June 2023: Under the lead of the EPPO in Cologne (Germany), law enforcement authorities in seven EU countries take action against an international organised crime group that operated a Missing Trader Intra-Community fraud scheme with cars. The operation results in over 450 searches as well as seizures of real estate and luxury cars; five people are arrested. The criminals used a buffer company in Germany and missing traders in Italy and Hungary. As a consequence, VAT of more than €38 million was evaded. The EPPO in Cologne conducts investigations for VAT fraud, tax evasion, organised crime, money laundering and forgery of documents.

■ 7/8 June 2023: The EPPO in Paris (France) has three people arrested for their involvement into a Europe-wide VAT fraud concerning the sale of second-hand cars. In addition, assets (Porsches, cash, Rolex watches, jewellery and luxury handbags), worth a total of more than €775 000, were seized. Bank accounts in Romania were frozen simultaneously. Investigations against the fraud scheme are also conducted in other participating EU Member States.

■ 5 June 2023: Three suspects are put under house arrest in Palermo (Italy) on suspicion of fraud in the context of renovations in a public school. The suspects are building constructors who received money from the EU Structural Fund for school renovation. However, they either attested work that existed only on paper or let carry out work by unqualified workers affecting the safety of the pupils and school staff. The Italian police also executed a freezing order of the financial assets of the building companies for a total amount of €140,000.

■ 2 June 2023: A manager of a Chinese company is put into pre-trial detention in Paris (France). He is considered responsible for concealing the true origin of electronic bicycles imports into the EU from China, thus evading the payment of taxes and circumventing EU trade measures against China in the sector of e-bikes. The EPPO in Paris conducts investigations for customs fraud and money laundering. The fraud scheme has also affected Czechia, Germany and Romania.

■ 29 May 2023: On behalf of the EPPO, the Lithuanian Financial Crime Investigation Service (FCIS) carries out raids in several Lithuanian counties and arrests 27 people. The action targets an organised criminal group that orchestrated a fraudulent scheme by which applications for project funding on behalf of young farmers were submitted, while there has never been the intention to implement the projects. The suspected organised group obtained more than €650,000 from national and EU funds for rural development.

■ 26 May 2023: The EPPO in Venice (Italy) has a freezing order of up to €171,000 executed against a company and four individuals in Trentino. The suspects are involved in "pasture fraud", i.e. allegedly having falsely claimed management rights to grazing lands in order to obtain subsidies from the EU's Common Agricultural Policy (CAP).

■ 25 May 2023: The EPPO in Zagreb (Croatia) reports that its investigations, which were launched on 14 July 2022 with regard to fraud into a waste water treatment plant project funded by the EU's Cohesion Fund (→eucrim 2/2022, 97), expanded. The investigations already led to the arrest of three suspects on 14 July 2022. According to new findings, one of the defendants ensured that the company of another defendant is included in the execution of works. In addition, there is suspicion that EU funds were used for private house renovation. The project involved a total of over €21 million of public grants.

■ 25 May 2023: The Guardia di Finanza in Palermo (Italy) executes a judicial freezing order of €20 million against three public officials and Palermo's water service company. The case, which was reported by the European Investment Bank (EIB) to the EPPO, concerns the undue receipt of public disbursement. During EPPO's investigations, the public officials are alleged to have deliberately ignored environmental regulations. Compliance with these regulations was, however, one of the requirements to receive a loan of €20 million from the EIB, funded by the European Fund for Strategic Investments (EFSI). The freezing order is to ensure the recovery of the damages to the EU budget.

■ 16 May 2023: In an investigation led by the EPPO in Bucharest (Romania) forty house searches are carried out in Romania and France. The investigation targets a criminal scheme in which fictious banks and dubious financial entities issued fake letters of guarantees to beneficiaries of EU projects. The guarantees are necessary to insure failure of services or contractual obligations by the beneficiary. The scheme also involves fictious banks/dubious financial entities in the Comoros Islands, Czechia, Latvia and Spain where fake letters of guarantees were issued and used in Romania. The fraud amounts to more than €30 million.

■ 12 May 2023: The Guardia di Finanza executes a judicial freezing order

issued at the request of the EPPO in Rome (Italy). The order targets an Italian company and their representatives which is suspected of having received undue financial support from the European Maritime and Fisheries Fund for the construction of mussel farming plants. It was revealed that the company's mussel farming facilities had already been entirely built and were operational before the application.

■ 11 May 2023: The EPPO in Turin (Italy) has money and real estate with a value of €530,000 seized from an agricultural company located in the Piedmont Region. The company and its managers are subject to investigations for unduly benefitting from an EU grant for the construction of rice dryers. Forensic analyses found that the requirements in the contract have actually been disregarded. The defendants are accused of aggravated fraud and embezzlement. The damage to the EU budget is over €500,000.

■ 9 May 2023: Upon request by the EPPO in Venice (Italy), the leader of an organised crime group is arrested. In addition, assets of more than €28 million are frozen. The arrested person is suspected of leading a criminal group which committed Missing Trader Intra-Community (MTIC) fraud with the purchase and sale of electronic products. For this purpose, the group established around 70 shell companies in Italy and many other EU countries. By evading the payment of VAT, the group sold the products at much lower prices on the market and achieved high illicit profits.

■ 5 May 2023: The EPPO in Madrid (Spain) has searches and seizures of assets carried out against a criminal organisation that dedicated its activities to subsidy fraud into agricultural funds. The organisation is suspected of having explored land parcels that are not in its possession, simulated property rights and falsified lease contracts in application for agricultural subsidies. In addition, the organisation sold the information to third parties enabling them to apply for subsidies. The estimated damage to the budget is at least €500,000.

■ 5 May 2023: The Guardia di Finanza seizes bank accounts and real estate in Calabria worth over €700,000 against seven suspects and their companies which are under an EPPO investigation into EU agricultural fraud. The sum corresponds to public money that the suspects received for organic farming. However, they submitted false declarations in order to meet the eligibility criteria. (TW)

### Overview of Convictions in EPPO Cases: May–September 2023

The following provides an overview of court verdicts in EPPO cases in the various participating EU Member States, as far as reported by the EPPO. It covers the period from 1 May to 30 September 2023 and continues the overview in →eucrim 1/2023, 19. The overview is in reverse chronological order.

■ 17 August 2023: A judgment by the the Regional Court in České Budějovice (Czechia) becomes final in which two individuals were sentenced to suspended prison terms, a financial penalty and a ban on receiving subsidies. They did not use EU funding for a declared project dedicated to the employment of young people. Furthermore, property obtained with the EU funds was transferred to one of the defendants. The damage of €125,000 was recovered during the EPPO proceedings.

■ 26 July 2023: A plea agreement concludes an EPPO case against the Deputy Mayor of Sibiu (Romania). The Mayor agreed with the penalty of two years and three months of imprisonment, suspended for a period of three years. In addition, he will perform community service for a period of 90 days. Investigations revealed that the defendant committed subsidy fraud during his previous position as director of a teacher's training centre. He used and presented several false and inaccurate documents and statements, with the intention to illegally receive funds of around €700,000.

■ 18 July 2023: The County Court of Zagreb (Croatia) convicts a Croatian farm owner for subsidy fraud and forgery of documents. The defendant obtained or claimed subsidies from the European Agricultural Fund for Rural Development (EAFRD) by disguising that he had not the financial means to implement proposed projects. He also hasn't made payments to suppliers, even though he declared them. The defendant was sentenced to 11 months' imprisonment, exchanged for community service and a fine of HRK 200,000 (€26 512). He also paid the damage to the EU and Croatian budget amounting to over €221,000. The sentence was based on a plea bargain.

■ 12 June 2023: The Regional Court of Ostrava (Czechia) confirms plea bargains by which two managers and two companies are convicted for subsidy fraud. EPPO investigations revealed that the managers deceived public authorities as to their criminal records, thus unduly receiving money for a employee-training project from the EU's Social Fund. The managers were sentenced to imprisonment on probation.

■ 31 May 2023: The High Court of Prague confirms a conviction of the Regional Court of Ústí nad Labem (Czechia) of February 2023. The courts convicted a company owner to 30 months of imprisonment with a probationary period of four years and a financial penalty of €8,500. Her company was prohibited from applying for and receiving subsidies for a period of six years. The company owner received over €70,000 from EU funds for leadership training of managers. EPPO investigations by the office in České Budějovice revealed that not managers were documented

participants, but taxi drivers, who had never attended any training session.

■ 10 May 2023: Following an indictment for illegal trade in cigarettes filed in January 2023 by the EPPO in Zagreb (→eucrim 1/2023, 22), the County Court of Zagreb convicts three out of six defendants on the basis of plea bargains. The defendants were found guilty for the illegal trade of cigarettes, tax or customs duty evasion and bribery, committed as part of a criminal organisation. The first and second defendant were sentenced to two years and eleven months of imprisonment, with a partial suspended sentence of one year and five months. The third defendant was sentenced to two years of imprisonment, with a partial suspended sentence of one year. "Partial suspended sentence" means that the remaining prison sentence as indicated will not be served, unless the convicted persons commit another criminal offence within a certain period of time (e.g. five or four years). In addition to the prison sentences, all three defendants are obliged to repay the damages they caused to the Croatian and EU budget (in total €3.07 million). The case involves the smuggling of cigarettes from Dubai to Croatia without paying taxes. (TW)

## Europol

### General Court: EDPS Action against Europol Regulation Inadmissible

On 6 September 2023, the General Court (GC) dismissed the action for annulment of parts of the new Europol Regulation brought by the European Data Protection Supervisor (EDPS) as inadmissible. The EDPS sought the annulment of transitional provisions (Arts. 74a and 74b) of Europol Regulation (EU) 2022/991 that entered into force on 28 June 2022 (→eucrim 2/2022, 98–100). The provisions confer on Member States the possibility to retroactively authorise Europol to process large data sets already shared with Europol prior to the entry into force of the amended Regulation. The EDPS considered these provisions contrary to his order of 3 January 2022 (→eucrim 1/2022, 18) requesting Europol to delete data concerning individuals with no established link to a criminal activity within a predefined, clear time limit because otherwise the principle of data categorization, enshrined in Europol Regulation 2016/794 would be infringed (Case T-578/22). For the EDPS's action for annulment →eucrim 3/2022, 177–178.

The EDPS argued before the GC that the European Parliament and Council, when adopting the amendments to the 2016 Europol Regulation, infringed the independence and powers of the EDPS as a supervisory authority, as a consequence of the infringement of the principle of legal certainty and of the principle of non-retroactivity of legal acts. Accordingly, the contested provisions retroactively legalised Europol's data retention practices and *de facto* annulled his decision of 3 January 2022.

The GC held, however, that the EDPS's action is inadmissible. The GC argues that the EDPS does not have a privileged standing before the CJEU, thus he must be treated in the same way as a "normal" legal person who must demonstrate that the EU act in question directly and individually concerns the person. According to the GC, this is not the case here because of, *inter alia*, the following reasons:

■ The EU act in question (amending the initial Europol Regulation) has no bearing on the nature or scope of the tasks entrusted to the EDPS who can continue to exercise his powers;

■ The EDPS decision of 3 January 2022 is an administrative decision which cannot affect legislative acts such as the amended Europol regulation or affect the content thereof;

■ The contested provisions leave discretion to Europol as to the analysis of personal data, and are thus not purely automatic in nature.

The EDPS appealed the GC's order before the ECJ. The appeal case there is referred as Case C-698/23 P. (TW)

### AG Opinion on Joint and Several Liability between Europol and Member States

In his opinion of 15 June 2023 in Case C-755/21 P, Kočner v Europol, Advocate General *Rantos* concludes that EU law has introduced a system of joint and several liability between Europol and the Member State concerned for damage suffered as a result of unlawful data processing as a consequence of action by Europol or that Member State. Hence, Europol and a Member State in which damage occurred in relation to unlawful data processing can be jointly and severally liable.

Opinions of Advocates General propose legal solutions to a case that are not binding for the Court of Justice. It is now for the judges of the Court to begin deliberations in this case. (CR)

### EDPS Opinions on International Agreements between Europol and Latin American Countries

The European Commission recommended opening negotiations for international agreements on the exchange of personal data to fight serious crime and terrorism between Europol and the competent authorities of five Latin American countries (Ecuador, Brazil, Peru, Bolivia, Mexico). At the beginning of May 2023, the EDPS issued a series of opinions in order to provide advice on further developing data protection safeguards in these agreements.

Among the suggestions, the EDPS recommends that the future international agreements explicitly list the criminal offenses and purposes for which individuals' personal data may be exchanged. They should also provide for periodic review throughout the time period in which transferred personal data is stored; appropriate

measures should be put in place to ensure that these time periods are respected. The agreements should explicitly exclude transfers of personal data obtained in violation of human rights. Lastly, in order to facilitate the enforcement of appropriate data protection measures, the parties involved in these international agreements shall exchange information on the following:

- The exercise of individuals' fundamental rights on a regular basis;
- The application of the relevant supervision and redress mechanisms.

When presenting the opinions, *Wojciech Wiewiórowski*, EDPS, added that "[p]articular circumstances of each foreign jurisdiction, such as existence of an independent data protection authority, or the accession to Convention 108 of the Council of Europe, should always be duly taken into account." (CR)

### Europol Updated Strategy Adopted

At the beginning of July 2023, the Europol Management Board adopted the agency's updated corporate strategy. The renewed strategy, "Delivering Security in Partnership", sets out six strategic priorities for Europol's mandate in the upcoming years, including highlights and examples:

- Be the EU criminal information hub, including for data acquisition;
- Deliver flexible, real-time operational support;
- Be a platform for European policing solutions;
- Bring the relevant partners together for cross-border cooperation and joint action;
- Be at the forefront of law enforcement innovation and research;
- Be the model EU organisation for law enforcement cooperation.

Under the renewed strategy, special priority is given to bolstering Europol's role in bringing together relevant partners for operational cooperation. To this end, Europol will especially invest in its partnerships with the Schengen-associated countries, Interpol, and key JHA agencies such as Frontex. Likewise, private parties, including companies, universities, NGOs and research institutes will be important partners. Interpol will continue to be an important bridge to countries around the world with which Europol does not have cooperation agreements. (CR)

## Eurojust

### Eurojust Annual Report 2022 – Criminal Justice Across Borders

At the end of May 2023, Eurojust published its Annual Report for the year 2022. While the past year was marked by responses to the unjustified invasion of Ukraine by Russia (→eucrim 1/2023, 11), Eurojust also provided support in 11,544 cases in 2022, the highest number for the agency ever:

- The total number of cases supported by the agency increased 14% compared to the previous year: 5227 cases were new cases and 6317 were ongoing cases from previous years;
- As in previous years, the majority of new cases concerned swindling and fraud (2028), drug trafficking (1054), and money laundering (1197);
- Eurojust contributed to the arrest of more than 4000 suspects, the seizure and/or freezing of criminal assets worth almost €3 billion, and the seizure of drugs worth almost €12 billion;
- It provided operational guidance on the application of EU judicial cooperation instruments, in particular with regard to the European Arrest Warrant (1262 cases) and the European Investigation Order (5415 cases);
- It provided assistance in 3333 mutual legal assistance cases;
- It assisted 78 new Joint Investigation Teams (JITs) and provided €1.91 million in JIT funding.

Overall, Eurojust continued to anchor the rights of victims in all its operational casework and helped deliver justice to more than 300,000 victims of all forms of serious, cross-border crime.

In 2022, the agency held international/cooperation agreements with 13 third countries and was actively connected with over 60 jurisdictions worldwide. It also actively cooperated with major players in the EU criminal justice area, such as Europol, OLAF, eu-LISA, FRA, and EUIPO. Furthermore, Eurojust signed a working arrangement with the Iberomerican Association of Public Prosecutors and expanded its Contact Point Network to include Australia, Bahrain, and Morocco.

Alongside various contributions to publications, conferences, and legal drafts, Eurojust also published the commemorative book "20 years of Eurojust: EU judicial cooperation in the making" last year. (CR)

### New National Member for Finland

At the beginning of August 2023, Ms *Heli Vesaaja* took took up her duties as new National Member for Finland at Eurojust. Prior to joining Eurojust, Ms Vesaaja was a member of the International Unit of the Helsinki Prosecutor´s Office. She also served as EJN Contact Point for many years. In addition to her career as prosecutor, Ms Vesaaja also held positions as a court lawyer at the European Court of Human Rights, as a magistrate in the European Anti-Fraud Office (OLAF), as a senior adviser for legislative matters with the Ministry of Justice in Finland, and as Seconded National Expert to the Directorate-General for Justice, Freedom and Security at the European Commission. Ms Vesaaja succeeds Ms Lilja Limingoja. (CR)

### First Liaison Prosecutor for Moldova

For the first time, the Republic of Moldova has stationed a liaison prosecutor at Eurojust. At the beginning of September 2023, Mr *Mihail Ivanov* took up this new position, with the

aim of strengthening cooperation between the Moldovan authorities and Eurojust in cases of serious cross-border crime. Prior to his secondment, Mr Ivanov served as interim deputy to the Chief Prosecutor of the Moldovan Anticorruption Prosecutor's Office. He has also held positions as contact point responsible for law enforcement issues with the Anti-Corruption Network for Eastern Europe and Central Asia of the OECD, as prosecutor in the Moldavian Anticorruption Prosecutor's Office, and as a military prosecutor for the Chisinau Military Prosecutor's Office. The posting of Mr Ivanov implements a Eurojust cooperation agreement with Moldova, which entered into force in October 2016. Cases at Eurojust involving Moldova have become increasingly important. (CR)

### New Liaison Prosecutor for Norway

At the beginning of September 2023, Mr *Rudolf Christoffersen* took up his duties as liaison prosecutor for Norway at Eurojust. During his career, Mr Christoffersen held positions as public prosecutor in Bergen, as deputy to the Norwegian Liaison Prosecutor at Eurojust, and as a member of the Group of Experts on Action against Trafficking in Human Beings (GRETA) with the Council of Europe. Mr Christoffersen succeeds *Christian Jordet* who held this position since August 2020. Norway has seconded liaison prosecutors to Eurojust since 2005 when the cooperation agreement between Norway and Eurojust came into force. Norway was the first third country that assigned a prosecutor to Eurojust.

Liaison Prosecutors are posted at Eurojust based on the international agreement with the respective non-EU country. The mandate and duration of each posting are determined by the national authorities of the respective country. Liaison Prosecutors have access to Eurojust's operational tools and facilities, including the use of office space and secure telecommunications services. (CR)

## European Judicial Network (EJN)

### 25th Anniversary of the EJN

The year 2023 marks the 25th anniversary of the establishment of the European Judicial Network (EJN) in criminal matters. The EJN was set up in 1998 by the Council of the EU with the aim of assisting judicial practitioners in combating cross-border crime. Since then, a network of approximately 450 contact points in EU Member States and beyond has been established to facilitate direct one-to-one contact in order to resolve legal issues and carry out preparatory work for judicial cooperation in criminal matters.

Additional support is available through the EJN website, which offers practical guidance via its tools like Judicial Atlas, Compendium, and Fiche Belges. In addition, the website includes information about national judicial systems. By means of the Judicial Atlas, the authorities competent to receive requests for judicial cooperation can be identified. The Compendium offers access to forms for EAWs and MLAs in all 24 official languages of the EU, together with e-tools to assist authorities in filling out, drafting, and sending the requests. Lastly, the Fiche Belges portal provides legal and practical information on the applicability of judicial cooperation measures.

The EJN is supported by a Secretariat and a rotating Presidency Board, which follows the rotation scheme of the Council of the EU. The Secretariat is hosted by Eurojust. In January 2023, *Hugh Dockry* from Ireland became Secretary to the EJN, succeeding Swedish *Ola Löfgren*. In numbers, the EJN registers ca. 8000 new reported cases and approximately 4 million website page views per year. (CR)

## Frontex

### Frontex Signs MoU with Albania

On 6 June 2023, Frontex and Albania signed a Memorandum of Understanding to strengthen their cooperation on the protection of fundamental rights in Frontex operational activities in Albania. Frontex and Albania had been using independent complaint mechanisms to deal with allegations of fundamental rights violations in Frontex operational activities on Albania's territory until now. The Memorandum builds a bridge now between these mechanisms to ensure that all those taking part in such operations respect and protect the fundamental rights of the persons crossing the borders. Under the Memorandum, Frontex is responsible for handling complaints related to alleged misconduct of the agency's officers, while Albanian authorities will handle complaints about misconduct of their staff.

The MoU is another step in the cooperation between Albania and Frontex. It was preceded by the launch of a joint operation in May 2019, by a renewed working agreement in March 2021 (→eucrim 1/2021, 18), and by a separate agreement on cooperation and information exchange of February 2022. (CR)

### 2022 Annual Report of the Frontex Consultative Forum

On 26 June 2023, the Frontex Consultative Forum on Fundamental Rights published its tenth annual report for the year 2022 (for the 2021 report →eucrim 3/2022, 180–181). The Frontex Consultative Forum brings together key European institutions as well as international and civil society organisations to advise the agency in fundamental rights matters.

In two main chapters, the report summarizes the fundamental rights advice given by the Consultative Forum in 2022 on the agency's operations and procedures. Regarding the

latter, the report closely looks at the support provided on the identification of vulnerable persons and on fundamental rights aspects of the European Travel and Authorisation System (ETIAS). In the area of operations, the Consultative Forum stepped up its operational fundamental rights advice by carrying out on-the-spot visits, with the objective of improving its operational understanding and tailoring future recommendations to the relevant operational context.

Although the year 2022 was marked by allegations of fundamental rights violations in Frontex-financed operations, the resignation of the Frontex Executive Director, and a series of remedial measures (→eucrim 3/2023, 181), the Consultative Forum also observed an increased effectiveness in the Frontex fundamental rights monitoring mechanism. This was particularly due to the findings and evidence collected by the Fundamental Rights Monitors, who were fully operational by the end of 2022. However, the Consultative Forum also sees a gap in relation to follow-up actions undertaken by Frontex regarding their recommendations and proposals for mitigating measures. Nevertheless, the Forum notes a positive development in the adoption of Standard Operating Procedures on decisions to suspend, terminate, or not launch activities (Art. 46 of Regulation (EU) 2019/1896).

Lastly, as a new Annex, the report released the Consultative Forum's expenses for the year 2022, which totalled €37,789.89. (CR)

### Frontex Fundamental Rights Officer Published 2022 Report

On 7 June 2023, the Frontex Fundamental Rights Officer published the Annual Report for the year 2022. It gives an overview of the Officer's monitoring and advisory activities performed in that year.

In six chapters, the Annual Report records the positive developments and main areas of concern and presents the results of fundamental rights monitoring conducted as part of the Agency's operational activities, including country-specific monitoring findings. In addition, it describes recent developments and provides a statistical overview of the number and type of serious incident reports and complaints received as well as information on capacity building activities. The cooperation of the Fundamental Rights Office with internal units of the agency, the Consultative Forum, and third countries is also outlined. Lastly, the report summarizes the recommendations issued in relation to Frontex by the Fundamental Rights Office (FRO) as well as the European Ombudsman, the Frontex Scrutiny Working Group of the European Parliament (FSWG), and the Working Group on Fundamental Rights and Legal Operational Aspects of Operations in the Aegean Sea (FRaLO) that are of relevance to fundamental rights.

The last chapter includes the FRO's planned actions and priorities for 2023:

- Enhancement of the team of Fundamental Rights Monitors through steady training and field experience as well as efficient deployment of all staff;
- Improved use of tools by, for instance, reinforcing established processes such as serious incident reporting, the complaints mechanism, and the Consultative Forum;
- Possible roll-out of new tools such as reporting tools for forced return and general monitoring;
- Work on the Fundamental Rights Action Plan, providing and following up on advice and opinions provided to the Management Board and Agency;
- Systematic tracking of response and action by national authorities in relation to serious incident reports.

The Fundamental Rights Officer is mandated with monitoring Frontex implementation of its fundamental rights obligations in accordance with EU and international law. This includes reporting on possible violations, promoting the inclusion of fundamental rights in the activities of the agency, and providing advice and recommendations. (CR)

### Frontex Published Risk Analysis 2023/2024

In its annual Risk Analysis for the year 2023/2024, Frontex provides a comprehensive overview of the challenges at the EU's external borders, especially irregular migration, secondary movements and returns as well as cross-border crime. According to the report, in 2022, about 332,000 illegal border-crossings at the EU's external borders on entry were reported by Member States, the highest number since 2016 (and +66% compared to 2021). Looking at the migratory routes, the report identifies the Western Balkan, Central Mediterranean, and Eastern Mediterranean routes as the top three routes used for illegal border-crossings. Syrian, Afghan, and Tunisian migrants attempted border crossings most often. At the same time, in 2022, a record number of people smugglers (over 15,000) were reported to Frontex.

In this context, the report underlines the need for effective deployment of the Standing Corps. Furthermore, it calls for new remedies to counter rising cross-border crime and migrant smuggling.

With regard to returns of third-country nationals, the report states that the gap between return decisions and effective returns could not be closed in 2022. According to Frontex, a common EU system for returns is needed. It also points to the Policy Document Towards an Operational Strategy for More Effective Returns that was issued in January 2023 and provides solutions for the digitalisation of return management as well as

the improvement of data and statistical evidence on return.

Looking ahead, the report expects a further increase in illegal migration to Europe in 2023/2024 considering the growing socio-economic push factors in numerous countries of origin. In light of Russia's continuing attack on Ukraine, the instrumentalization of migrants by Russia and Belarus is likely. Ultimately, the situation may be a driver for organised cross-border crime, especially the smuggling of drugs, tobacco, and illicit goods. Europe's current labour shortage may also lead to increased trafficking in human beings for labour exploitation purposes. Unaccompanied minors arriving at Europe's external borders are another concern. (CR)

### Pilot Project on Command Structure Launched

In mid-June 2023, Frontex and Romania launched a new operational pilot project at Romania's external border with Moldova and Ukraine. The project aims to test a new command structure in order to further strengthen the effectiveness of Frontex operations. The growing number of officers deployed by the agency requires new steps to be taken to reinforce its command in the field and to decentralise some of its activities for better coordination and communication with host country authorities. National authorities remain responsible for the tactical command tasks in the respective operational areas. In 2024, the plan is to implement the new command structure in all Frontex operations. (CR)

### Joint Action Days Against Cross-Border Crime

A weeklong operation took place at the end of June 2023, involving 12 EU and EU-associated countries in Central and South-Eastern Europe, Frontex, Eurojust, Europol and INTERPOL. The international operation led to the arrests of 108 people smugglers. It was conducted by Frontex standing corps officers, along with customs officials, border guards, and police officers from the participating countries. The focus was on combatting the smuggling of migrants, fighting trafficking in human beings, and on document fraud. During the operation, 65 million border checks were performed, 115 false documents detected, and 25 stolen vehicles seized.

The operation was part of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) – a recurring four-year cycle to identify, prioritise, and address threats posed by organised and serious international crime. (CR)

## Agency for Fundamental Rights (FRA)

### Report on the Protection of Human Rights Defenders

On 11 July 2023, the Agency for Fundamental Rights (FRA) published a report examining the opportunities for human rights defenders from third countries to enter and stay in EU Member States, including good practices and ways to improve the situation. The report, which was drafted on the request of the European Parliament, is based on input from the Agency's multidisciplinary research network "Franet", expert interviews, secondary research, and consultations with relevant stakeholders.

To assess the situation, the report examined how existing relocation programmes function for human rights defenders as regards their entry into and stay in the EU, including visas and residence permits. It also focused on the obstacles they face, including the type of support defenders need and receive once relocated. Annex I of the report provides a table listing Member States' practices in this respect.

According to the report, the current situation in the EU is characterised by a patchy and complex system: different types of visas used for this specific group of people, varying relocation practices across the EU, and scant support for longer-term stays in the EU. As a result, the report sets out six points for consideration by the EU and its Member States to improve the situation for human rights defenders:

- Better and more frequent recourse should be taken to the existing flexibility in EU law. For instance, access to short-stay visas should be facilitated by applying the existing exceptions and derogations in the EU Visa Code. The European Commission could compile a dedicated catalogue of the various options available for this purpose;
- The EU Member States could broaden the scope of their relocation programmes or, where not yet available, introduce such programmes;
- Awareness about human rights defenders could be improved, both in their home countries and while in relocation;
- The benefits and risks of digitalisation and the use of technology impacting on human rights defenders' opportunities to come to the EU should be taken into account;
- During their stay, increased and adequate support should be provided that goes beyond the provision of visa and residence permits, with the aim of enabling the defenders to effectively continue their human rights work;
- The EU should ultimately review the adequacy of its legal tools for supporting human rights defenders, especially the Visa Code, the Visa Information System (VIS) Regulation, the European Travel Information and Authorisation System (ETIAS) Regulation and the Entry-Exit System Regulation , and also suggest possible amendments, if necessary.

FRA emphasised that, in general, any support and protection instrument for human rights defenders should serve to ensure the safety, integrity and dignity of human rights defenders

and their family members as well as to support their ability to continue their human rights work. (CR)

### European Data Protection Supervisor

#### Adapting to New Challenges: Organisational Changes within the EDPS

On 10 July 2023, the European Data Protection Supervisor (EDPS) announced several organisational changes, with the aim of ensuring structural efficiency in the protection of personal data and privacy in a fast-changing environment. To achieve this, the EDPS has created the new position of Secretary-General. The Secretary-General heads the EDPS Secretariat, oversees the EDPS' activities, and provides strategic advice to the EDPS. The first Secretary-General appointed by the EDPS is Mr *Leonardo Cervera Navas*. Mr Cervera Navas has more than 24 years of work experience in the field of data protection within EU institutions, having last held the position of EDPS Director.

In addition, the EDPS has created specific sectors to monitor the EU's Area of Freedom, Security and Justice; to address complaints made by individuals and launch timely investigations into the way personal data is processed by EU institutions and bodies (EUIs); and to deliver comprehensive advice to EUIs on data protection matters. Furthermore, the Technology and Privacy Unit has been redefined with the establishment of new sectors to ensure that technologies embed the principles of privacy and data protection: a specialised sector to ensure thorough oversight and auditing of IT systems; a sector to anticipate new technologies and their impact on privacy and data protection; and a sector to develop the independent digital transformation of the institution. Lastly, a task force on the use of artificial intelligence has been set up to ensure that this technology is used in full respect of data protection law. (CR)

## Specific Areas of Crime

### Financial and Economic Crime

#### Europol Published First Threat Assessment on Financial and Economic Crime

**spot light**

At the beginning of September 2023, Europol published a threat assessment on financial and economic crime. It is the first Europol threat assessment report in this criminal area. Under the title "The other side of the coin: an analysis of financial and economic crime in the EU", the report deals with all financial and economic crimes affecting the EU, such as money laundering, corruption, fraud, intellectual property crime, and commodity and currency counterfeiting.

In the first chapter, the report looks at today's drivers of financial and economic crimes (e.g. serious and organised crime), the digital acceleration of society, and geopolitical developments. The second chapter analyses the engines of crime, namely money laundering, criminal finances, and corruption. The third chapter explains the world of fraud by giving examples of investment fraud, business e-mail compromise (BEC), e-commerce fraud, tech support fraud, romance fraud, scams, mass mailing, and food fraud; it also explores the range of different fraud schemes against the financial interests of the EU and Member States, such as VAT fraud and fraud schemes linked to sporting events.

Chapter four is dedicated to intellectual property crime (IPC) and counterfeiting, explaining which commodities and factors are most affected by IPC as well as the methods of currency counterfeiting. The final chapter summarises the responses to these threats, including the establishment of Europol's European Financial and Economic Crime Centre (EFECC), Europol's Financial Intelligence Public Private Partnership (EFIPPP), and cooperation with other bodies and agencies, such as the European Anti-Fraud Office (OLAF), the European Public Prosecutor's Office (EPPO), and the European Union Intellectual Property Office (EUIPO).

In numbers, the report states that almost 70% of criminal networks operating in the EU make use of one form of money laundering or the other to fund their activities and conceal their assets. Furthermore, more than 60% of the criminal networks operating in the EU use corrupt methods to achieve their illicit objectives. Lastly, 80% of the criminal networks active in the EU misuse legal business structures for criminal activities. Asset recovery is seen as one of the most powerful and effective deterrents by which to tackle serious and organised crime. Yet the amount of captured proceeds still remains too low – below 2% of the yearly estimated proceeds of organised crime.

In conclusion, the report underlines the role of corruption and money laundering as linked in the licit and illicit financial and economic worlds. Corruption and money laundering threaten to erode trust in authorities, in the rule of law, and in the general functioning of society. Due to the limited degree of recovery of criminal assets, the problem of laundered illegal profits being invested in the licit economy, and the victimisation of millions of EU citizens in different fraud schemes, financial and economic crimes pose a serious threat to the EU's internal security. For this reason, financial investigations should become standard law enforcement practice when investigating serious and organised crimes. Because of their specific external dimension, the report calls for a multidisciplinary and comprehensive approach towards tackling these types of crime affecting the EU. (CR)

## Protection of Financial Interests

### 34th Annual PIF Report

spot light

On 27 July 2023, the European Commission adopted the 34th Annual Report on the protection of the European Union's financial interests and the fight against fraud in 2022. For the first time, the report is not only made available in a PDF format but also in a digital version that provides additional information through hyperlinks and built-in content. The report provides information on:

- The key measures to prevent and fight fraud at the EU level;
- Member States' measures to protect the EU's financial interests;
- Data on and analytical findings of irregularities and fraud reported by the Member States, including information on OLAF and EPPO investigations;
- Conclusions and recommendations.

The report underlines progress in the overall coherence of anti-fraud legislation across the EU. A key factor for this is the ongoing correction of problems in the transposition of EU rules into national systems. 24 Member States have a strategy in place to increase the protection of the EU's financial interests or are in the process of finalising one. The revision of the Financial Regulation that is currently under discussion will bring improvement, the report writes, in particular as regards better transparency in the use of the EU funds, digitalisation of the fight against fraud and fraud risk management.

Further digitalisation is a key point to ensure more effective and efficient fraud prevention and detection. This is also included in the Commission's Anti-Fraud Strategy which will be followed up in the future.

Regarding the key figures, the report states that the number of cases of fraud and irregularities reported by the competent EU and national authorities – 12,455 in total – slightly increased in 2022 compared to 2021 (+7%). By contrast, the irregular amounts related to these cases decreased to €1.77 billion (–13%).

According to the report, detection and reporting of suspected fraud and irregularities can still be improved, as can their follow-up. There are still significant differences between Member States. It is recommended that those Member States with low incidence of fraud should invest in fraud risk analysis in order to assess as to whether low detection is the result of low levels of actual fraud or the result of systemic weaknesses in detection or reporting systems. Member States should also address more carefully the question of "intentionality" so that fraudulent practices can be better detected. Moreover, Member States should review reporting practices. Further recommendations include the following:

- Ensuring that the digitalisation of the fight against fraud is part of the national anti-fraud strategies. Such strategies should include: (i) identification of existing and future threats arising from new technologies; (ii) development of the necessary IT architecture; and (iii) identification and remedy of existing gaps, also in terms of the skills needed.
- Extending national anti-fraud networks with the aim to involve all the relevant law enforcement and judicial authorities as well as proper staffing of the national anti-fraud structures.

As in the previous years, the annual report on the protection of the EU's financial interests is accompanied by several other documents, including:

- Annex with the number of non-fraudulent and fraudulent irregularities reported by each Member State in 2022;
- Annual overview with information on the results of the Union anti-fraud programme in 2022;
- Activity report of the EDES Panel;
- Follow-up by the Member States on the recommendations of the PIF Report 2021;
- Measures adopted by the Member States to protect the EU's financial interests in 2022 (implementation of Art. 325 TFEU);
- Statistical evaluation of irregularities reported for 2022 (own resources, agriculture, cohesion and fisheries policies, pre-accession and direct expenditure).

For the annual reports of previous years →eucrim 3/2022, 182–183 and the related links there. (TW)

### ECJ: EU Law Protecting the Union's Financial Interests Prevails over National Fundamental Rights

spot light

In its judgment in *Lin* (Case C-107/23 PPU) of 24 July 2023, the ECJ clarified the obligations of Member States arising from the need to combat fraud affecting the financial interests of the Union and the need to respect fundamental rights protected by EU law and national law.

➤ *Background of the case and AG's opinion*

The ECJ had to rule on a reference for a preliminary ruling from the Romanian Court of Appeal in Brașov. In 2010, the appellants in the main proceedings had failed to declare commercial transactions and income relating to the sale of diesel fuel, thereby causing a loss to the state budget. In June 2020, the Court of Appeal sentenced the concerned persons to terms of imprisonment for tax evasion and the setting up of a criminal organisation. In addition, they were ordered to pay €3.2 million in compensation.

In their appeal, the concerned persons argued that a conviction was no longer possible because the limitation period for criminal liability of the offences had expired. They based their appeal on the principle of the retroactive application of the more lenient criminal law *(lex mitior)*. Specifically, provisions pertaining to the limitation period for criminal liability had been declared unconstitutional by the *Curtea Constituțională* (Constitutional Court)

in judgment No. 297/2018 as they violated the principle of legal certainty of criminal offences and penalties. This was upheld in judgment No. 358/2022 in light of the inaction of the Romanian legislature. In consequence, Romanian law lacked applicable grounds for the interruption of the limitation period for criminal liability, i.e. by procedural acts or decisions. Following this interpretation, the ten-year limitation period provided for in the Romanian Criminal Code would have expired before the concerned persons' convictions had become final. This would mean that the criminal proceedings would have to be discontinued and that the concerned persons could not be sentenced.

In essence, the Romanian Court was asking whether this interpretation, which would have the effect of exonerating the concerned persons from criminal liability for serious fraud to the detriment of the Union's financial interests, is compatible with EU law. It also posed the question whether it might be obliged to declare the judgments of the Romanian Constitutional Court inapplicable in the event that an interpretation in conformity with EU law were not possible. However, under Romanian law, judges who disapply case law of the Constitutional Court of their own motion risk committing a disciplinary offence.

In his opinion of 29 June 2023, AG *Sánchez-Bordona* advised that the EU's financial interests should not be protected at the expense of fundamental rights, such as the principle of retroactivity of the most favourable criminal law. Therefore, the referring court should not have to disapply the case law of the Constitutional Court in order to ensure conformity with Art. 325(1) TFEU and Decision 2006/928. This ensures compliance with the principle of criminal legality and the requirements of foreseeability and precision of the applicable criminal law.

➤ *The ECJ's ruling*

The ECJ took a different approach to the balance between the protection of the Union's financial interests and fundamental rights than the AG. Following the case law in *Euro Box Promotion and Others* (C357/19, et al.), the Court emphasised that a systemic risk of impunity is incompatible with the requirements of Art. 325(1) TFEU and Art. 2(1) of the PIF Convention. The Constitutional Court cases of 2018 and 2022, following which the national legislature has failed to remedy the situation for a period of almost four years, constitute such a risk, since numerous cases of serious fraud to the detriment of the EU's financial interests will remain unpunished because of the expiry of that limitation period. Therefore, in principle, the national courts are required to disapply judgments No. 297/2018 and No. 358/2022 of the Romanian Constitutional Court. It follows that Romanian law does not provide for any grounds for interrupting the limitation period for criminal liability between 2018 and 2022. Although such a result would lead to a restriction of the national standard of protection *(lex mitior)*, the application of these rules would undermine the primacy, unity, and effectiveness of EU law. As a consequence, EU law should therefore be given priority and the rulings of the Romanian Constitutional Court should not be applied.

On the judges fears of facing consequences for disregarding the Constitutional Court, the ECJ ruled that the non-application of the Constitutional Court's rulings may not lead to disciplinary proceedings against the judges. This would *ipso facto* violate the judgment and the principles it addresses. (SH)

### ECJ Ruled on Concept of "Irregularity" and Extent of Financial Corrections

In its judgment of 8 June 2023, the ECJ clarified the extent to which the Member States must recover European Union structural funds if there is merely a suspicion of corruption in the award of public contracts financed with them, where the suspicion is, however, substantiated by the initiation of administrative or judicial proceedings.

➤ *Facts and problem of the case*

The underlying case (*Case C-545/21, ANAS v Ministero delle Infrastrutture e dei Trasporti*) is as follows: The European Commission approved the national operational programme "Networks and Mobility" 2007–2013. Azienda Nazionale Autonoma Autostrade SpA (ANAS), as a beneficiary of this programme, was granted funding, *inter alia*, for the implementation of a project to modernize roads and, as contracting authority, carried out a call for tenders. After the Italian Ministry of Infrastructure and Transport became aware of a criminal investigation that brought to light a potential system of corruption involving ANAS officials (*inter alia*: prosecution for bribery of two members of the five-member procurement committee in connection with the award decision), it ordered the recovery of the amounts already paid to ANAS under this programme. It also declared that the remaining amount not yet paid should not be paid, as it was to be assumed that an irregularity of a fraudulent nature had occurred in the award of the contract in question.

The Regional Administrative Court of Lazio dealing with ANAS's action against the Ministry's recovery decision had doubts as to whether and, if so, to what extent the Member State's obligation to recover EU funds exists if the award decision is not demonstrably attributable to the irregularity (corruption), the work funded was correctly carried out and it has not been established that the contractor obtained the public contract unlawfully.

➤ *The ECJ's ruling*

Thematically, the procedure is based on the obligation of the Member States to make the necessary

financial corrections in the event of irregularities in connection with European structural funds (cf. the then applicable Art. 98 of Regulation No 1083/2006 laying down general provisions on the European Regional Development Fund, the European Social Fund and the Cohesion Fund). The ECJ interprets the term "irregularities" as a factual element for the Member State's obligation to recover funds in a uniform and broad manner.

The ECJ reaches this conclusion by interpreting the three conditions of "irregularity", which are derived from the legal definition in Art. 2(7) of Regulation 1083/2006 and Art. 1(2) of Regulation 2988/95:

- An infringement of Union law;
- An act or omission by an economic operator which caused that infringement;
- An actual or potential prejudice to the Union budget.

Of the three conditions, the second and third conditions could be affirmed relatively easy and in line with previous case law. Thus, the ECJ considered ANAS to be an economic operator (second condition) and confirmed its case law that an "act or omission" requires neither intent nor negligence. In the case of "prejudice to the Union budget" (third condition), it is also sufficient that effects on the Union budget cannot at least be ruled out (cf. ECJ, judgment of 1 October 2020, Case *C-743/18 – Elme Messer Metallurgs*).

However, it had to be decided for the first time whether the (procurement) law infringement must actually have had an impact on the award decision (first condition). The ECJ answered this in the negative. It is sufficient that, due to the corruption allegations, it cannot be ruled out that the accused members of the ANAS procurement committee violated the public procurement law principles of "transparency" and "equal treatment of tenderers" within the meaning of Directive 2004/18 on public procurement for public works, supplies and services contracts .

With regard to the extent of the recovery, the ECJ ruled that the necessary financial correction must be determined on a case-by-case basis in accordance with the principle of proportionality, taking into account in particular the nature and seriousness of the irregularity and the financial impact on the fund concerned. However, a suspicion of fraud could be classified as "serious", so that a financial correction of 100% could be applied.

➤ *Put in focus*

The ANAS judgment makes it clear that a financial correction does not require that the irregularity has demonstrably influenced the award decision and corresponds to the financial impact on the fund. Even the suspicion of a breach of public procurement rules can trigger a recovery obligation. The ECJ clearly decides in favor of the effective protection of the Union's financial interests. The Member States' obligation to recover must not be undermined by problems of proof.

The relevant legal provisions examined have now been replaced. However, the ECJ's judgment is equally transferable to the comparable provisions of the successor regulation (see e.g. Art. 143 and Art. 2(36) of Regulation (EU) No 1303/2013) as well as to the new Public Procurement Directive 2014/24/EU. (TW)

### EP Grants Discharge but Raises Concerns over Attacks to EU Budget

On 10 May 2023, the European Parliament (EP) granted discharge to the EU institutions for the financial year 2021. The discharge for the European Council and the Council was postponed. The postponement continues the dispute between the EP and the Council with the latter continuously refusing parliamentary scrutiny over its annual financial implementations. The EP is set to refuse discharge for the European Council and Council for the 13th year in a row. For the first time, the EP discharged the European Public Prosecutor's Office since its operational start in June 2021.

In its discharge decision for the Commission and the executive agencies, the EP voiced numerous concerns over the effective protection of the EU's financial interests. One of the main concerns relate to the risk of misuse, fraud and organised crime within the scheme of the Recovery and Resilience Facility (RRF). MEPs pointed out that its is unclear how the money of the RRF is used; control requirements are weaker compared to traditional EU programmes and controls are more or less in the hands of national authorities whose work has proved "too error-prone and unreliable". MEPs called for "efficient internal control systems ensuring compliance with all Union and national rules, including, in particular, public procurement and state aid rules, and rules to prevent and detect fraud, corruption, conflicts of interest and double-funding".

MEPs were also concerned by "first indications" that in some EU countries RRF funds may be used to replace regular national expenditure rather than for the reforms and investments set out in national RRF plans. They also criticised that the definition of milestones and targets (a prerequisite for EU countries to receive RRF payments) was based on "political negotiations" and lack clear and fixed criteria.

MEPs stressed that the Commission must trigger without delay the application of the conditionality mechanism whenever breaches of the principles of the rule of law are identified to be affecting or are in serious risk of affecting the sound financial management of the Union budget. They welcomed the first application of the conditionality mechanism in the case of Hungary; however, facts would have justified the freezing of 100% of EU funds instead of the freezing of 55%

of three cohesion policy programmes (around €6,35 billion).

Further political priorities relate to NGOs. The EP calls for an effective mechanism to assure NGOs' activities are aligned with Union values and demand full transparency on their financing. A public black list should be created for NGOs, that have engaged in activities such as hate speech, incitement to terrorism, religious extremism supporting or glorifying violence, or have misused or misappropriated Union funds, in order to ensure they are blocked from access to Union institutions and Union funding programmes. In addition, the Commission is called to propose a new "NGO Regulation" that sets conditions for receiving EU funds and obligations to report sources of funding as well as activities performed on behalf of foreign actors. (TW)

### New Drive in the Debate on Own Resources

On 20 June 2023, the Commission adjusted and complemented its 2021 proposal to establish new own resources for the EU budget (→eucrim 2021, 213–214). The initiative (document: COM(2023) 331) comes after the Council had not shown much willingness to proceed with the legislative process. In addition, the European Parliament (EP) also pushed ahead the debate. In a resolution of 10 May 2023, the EP proposed an array of new own resources and other revenue sources for the EU budget, including corporate tax-based own resources, the financial transaction tax, a tax on crypto-assets, and national contributions based on statistics. One of the main reasons for new own resources is to cover the costs for the NextGenerationEU – the EU's economic package to recover from the COVID-19 pandemic (→eucrim 3/2021, 151).

The Commission now proposes a new statistical own resource based on company profits. It will be a national contribution paid by Member States based on the gross operating surplus for the sectors of financial and non-financial corporations. The Commission stressed that this contribution is not a corporate tax and it will be temporary until the "Business in Europe: Framework for Income Taxation (BEFIT)" is proposed and unanimously agreed by the EU Member States.

In addition, the Commission proposed adjustments to two elements of its 2021 proposal: the own resources based on the Emissions Trading System (ETS) and the Carbon Border Adjustment Mechanism (CBAM).

The Commission expects that these modifications can deliver on average €36 billion (2018 prices) per year as of 2028.

According to Art. 311 TFEU, any provision relating to the system of the EU's own resources requires a unanimous agreement by all EU Member States in the Council following a consultation of the EP. In addition, EU countries have to approve the agreement at national level, in accordance with their respective constitutional requirements. (TW)

### EU Commission Presents Package of Measures to Reinforce the Long-Term Budget

On 20 June 2023, the Commission tabled proposals for a targeted revision of the multiannual financial framework (MFF), which was adopted in 2020. Given the drastic global changes since then with economic and social effects (particularly following Russia's invasion of Ukraine), the Commission sees no alternative to additional financing in order to deliver on the EU's objectives. The reinforcements mainly include:

- Establishment of the Ukraine facility, based on grants, loans and guarantees, with an overall capacity of €50 billion in the period 2024–2027 to cater for Ukraine's immediate needs, recovery and modernization;
- Creation of the Strategic Technologies for Europe Platform (STEP) to promote the EU's long-term competitiveness on critical technologies in the fields of digital and deep tech, clean tech and biotech. STEP will build on existing programmes, but should also receive an additional €10 billion;
- Reinforcement of the EU budget by €15 billion to address internal and external dimensions of migration and to strengthen global partnerships;
- A new "EURI instrument" would cover the increased NextGenerationEU funding costs.

Moreover, the EU administrative capacity will be adjusted to cater for the new tasks that have been decided by the co-legislators since 2020 and to meet inflation-adjusted contractual obligations.

*Next steps:* The Commission proposals need to be adopted by the Council; the European Parliament must give its consent.

The Council started negotiations on the mid-term review of the MFF already in July 2023. The EU leaders held an in-depth discussion at the European Council meeting in October 2023 and invited the Council to take forward the work with a view to reaching an overall agreement by the end of the year. (TW)

### ECA: Digital Administration of EU Funds is Progressing Too Slowly

Bodies managing EU funds still face several challenges with the use of digital tools. Such shortcomings have an impact on the effective protection of the EU's financial interest. This is one of the main conclusions in a report presented by the European Court of Auditors (ECA) on 6 July 2023. The review report describes and analyses the current state of digitalisation in the management of EU funds as well as planned developments.

According to the ECA, digitalisation has the potential to make the audit of EU funds more efficient. However, because the multiple bodies managing EU funds use so many divergent IT systems, it is currently impossible

to undertake large-scale testing. The ECA also states that modernising the Commission's financial management system is a big challenge, a "truly digitalised Commission" is still work in progress. Weaknesses in the digitalisation of managing EU funds include:

- Lack of a corporate system for the Commission's indirect management needs;
- Considerable differences between Member States as regards the use of IT in the shared management areas, in particular cohesion policy and rural development funding, which makes an efficient exchange of information difficult;
- Uneven uptake of electronic procurement across Member States;
- Multiple databases and portals containing information on transparency of contractors and beneficiaries of EU spending, which additionally varies by management mode and policy;

Differences in data governance with some essential data still being unstructured or only available directly from managing authorities or beneficiaries, and thus unsuitable for digital audit and comprehensive analysis.

The ECA points out that it will be necessary to simplify the IT landscape still further in order to streamline the management of EU funds. Therefore, differences must be reduced and interoperability between IT systems and the data used by the many implementing bodies be improved. (TW)

## Corruption

### Commission Presents Anti-Corruption Package

On 3 May 2023, the Commission presented an anti-corruption package. This consists of the following:

- A joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy on the fight against corruption (JOIN(2023) 12 final). On the one hand, the Communication provides an overview of existing EU legislation and measures in the area of anti-corruption and on the other contains considerations on how future EU measures in this area could be strengthened. In this respect, the establishment of an EU anti-corruption network is planned;
- A Commission proposal for a directive on combating corruption (COM(2023) 234 final). The future directive is intended to update the existing EU anti-corruption framework, including Directive (EU) 2017/1371, by establishing minimum rules for the definition of criminal offenses and sanctions in the area of corruption and measures to better prevent and combat corruption;
- A proposal from the High Representative of the Union for Foreign Affairs and Security Policy for a new sanctions regime in the context of the EU's foreign and security policy (CFSP). This would allow the EU to take restrictive measures (EU sanctions) where acts of corruption seriously undermine or threaten to undermine the objectives of the CFSP. The proposal complements and strengthens the EU's other anti-corruption instruments.

The Commission's proposal for a directive on combating corruption will be discussed by the European Parliament and the Council. The proposed new framework for CFSP sanctions against corruption must be discussed and adopted by the Council.

The Joint Communication and the proposal for a new anti-corruption directive are analysed in separate news items. (TW)

### Commission and HR Set Out EU Action against Corruption

As part of the anti-corruption package presented on 3 May 2023, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (HR) outlined the risks of corruption to society, democracies, economy and individuals. In their Joint Communication on the fight against corruption (JOIN(2023) 12), they point out that even conservative estimates suggest that corruption costs the EU economy at least €120 billion per year. 69% of EU citizens believe that high-level corruption is not pursued sufficiently by national authorities and around half of businesses think it is unlikely that police or prosecutors will catch those engaged in corruption activities. The Communication stresses that the EU is constantly committed to prevention, maintaining a culture of integrity and the active enforcement of anti-corruption legislation, including effective prosecution of corruption crimes. This approach is also reflected in the EU' external action on anti-corruption underpinned by support to the rule of law and public financial management of partner countries. The latter aspect is to be reinforced in the future, including the HR's proposal for establishing a dedicated CFSP sanctions regime to fight corruption when and where acts of corruption seriously affect or risk affecting the fundamental interests of the Union and the objectives of the CFSP as set out in Art. 21 TEU.

The Communication provides an overview of the EU anti-corruption framework and how anti-corruption can be further mainstreamed into EU policy design. Several workstreams are identified, which represent major EU commitments to further make efforts in the prevention of and fight against corruption. These include:

- Building a culture of transparency and integrity;
- Preventive policies to address corruption risks;
- Detecting corruption;
- Cracking down on corruption.

Furthermore, the Communication outlines how the EU supports the fight against corruption in the EU Member States and within the EU institutions. It reflects on the "whole-of-society" approach, where close and regular coor-

dination with all relevant public authorities, multilateral organisations, civil society, media and the private sector is deemed essential. The last section of the Communication is dedicated to anti-corruption in the EU's external policies. Next to the aforementioned use of CFSP sanctions to target corruption, details are explained on anti-corruption in the EU's enlargement and neigbourhood policies, the promotion of anti-corruption reforms in the EU's external action and trade relations, and the support of anti-corruption work in multilateral fora.

One of the most important future steps is the extension and deepening of the EU network against corruption. The network will be designed as a catalyst for corruption prevention efforts across the EU. It will be tasked to develop best practices and practical guidance in various areas of common interest. In addition, it is to support a more systematic gathering of data and evidence that can serve as a solid basis for anti-corruption actions and for monitoring the success of these actions. The network is also invited to map common high-risk areas of corruption by 2024.

The Joint Communication is not yet a new, comprehensive EU strategy against corruption. However, the Communication and the work of the EU network against corruption will feed into this strategy. According to the Communication, the EU strategy against corruption "needs to be developed on a strong foundation of consensus and broad consultation, in particular with the European Parliament and Member States." (TW)

### Commission Proposes New Anti-Corruption Directive

**spot light**

On 3 May 2023, the Commission tabled a proposal for a directive which would establish new rules on combating corruption in the EU. The directive is set to replace Council Framework Decision 2003/568/JHA that lays down requirements on the criminalisation of corruption concerning the private sector, and the 1997 Convention on the fight against corruption involving EU officials or officials of EU Member States. It would also amend the PIF Directive (Directive 2017/1371).

In the explanatory memorandum, the Commission set out the reasons for this new legislative initiative:

- Previous calls by the European Parliament and Council for more EU action to combat corruption;
- Need for an update of the existing EU legal framework on combating corruption taking into account the evolution of corruption threats and the legal obligations on the Union and Member States under international law as well as the evolution of national criminal legal frameworks;
- Enforcement gaps at national level and obstacles in the cooperation in corruption cases between the competent authorities in different Member States;
- Addressing failings in integrity, undisclosed conflicts of interests or serious breaches of ethical rules that can lead to corrupt activities.

The draft directive combines preventive and repressive anti-corruption elements in one single EU act. It takes up provisions of the United Nations Convention Against Corruption (UNCAC) while at the same time going beyond international obligations in certain aspects. The directive includes several obligations for Member States that are based on three major pillars: prevention of corruption, harmonisation of the criminal law regarding corruption offences, better law enforcement . The main obligations and contents are summarised in the following:

➤ *Prevention of corruption*

- Raising awareness of corruption by carrying out information and awareness-raising campaigns, research, and education programmes;
- Ensuring the highest degree of transparency and accountability in public administration and public decision-making;
- Putting in place key preventive tools, including effective rules on access to information, on conflicts of interests in the public sector, on assets of public officials and their interaction with the private sector;
- Performing regular assessments to identify the sectors most at risk of corruption;
- Setting up specialised anti-corruption bodies and ensuring adequate resources and training for authorities responsible for preventing and fighting corruption.

➤ *Harmonisation of criminal law*

- Clarifying the definitions of and penalties for corruption offences;
- Making all offences under the UNCAC mandatory under EU law and bringing together public and private sector corruption;
- Covering the full range of corruption offences and extending the list (beyond the more classic bribery in the public and private sector) to: misappropriation, trading in influence, abuse of functions, obstruction of justice and illicit enrichment from corruption offences;
- Establishing consistent penalty levels for natural persons and setting standards for the liability of and sanctions for legal persons;
- Harmonising aggravating and mitigating circumstances.
- *Enforcement aspects*
- Defining minimum limitation periods for corruption offences that allow for sufficient time to effectively investigate, prosecute, trial and decide on corruption offences;
- Ensuring that privileges and immunity can be lifted during corruption investigations through an effective and transparent process pre-established by law, and in a timely manner;
- Ensuring that national law enforcement and prosecutors have appropri-

ate investigative tools to fight corruption.

Lastly, the draft directive also includes a provision to have better statistical data on corruption offences. The provision lists, in a non-exhaustive manner, the statistical data that should be collected by the Member States and obliges them to publish such data annually.

The next step is to negotiate the anti-corruption package in the EU Parliament and Council.

The proposal for a new anti-corruption directive is a core initiative that came in parallel with the presentation of other anti-corruption tools, including a Communication on combating corruption and a proposal for establishing a dedicated CFSP sanctions regime to target serious acts of corruption worldwide (→news items above). (TW)

### German Lawyer Associations Voice Concerns over Commission's Anti-corruption Directive

The proposed anti-corruption directive faces initial criticism by stakeholders. In September 2023, both the German Federal Law Society (*Bundesrechtsanwaltskammer, BRAK*) and the German Bar Association (*Deutscher Anwaltverein, DAV*) emphasised that the Commission's draft (→see previous news item) disregards the principles of proportionality and subsidiarity and warned that the proposal could restrict the sovereignty of the Member States in shaping their criminal law.

Both associations particularly criticized the definitions of "public officials" and "national officials", as they extend the protection of public services far beyond the level currently applicable in Germany and the EU as well as the lack of coherence with Directive 2017/1371 on combating fraud to the Union's financial interests by means of criminal law. In addition, the draft directive lacks clarity and vagueness of breaches of duty in the area of duty-related offenses in the proposal. The objection here is that benefits could be included that are promised in return for almost any breach of duty, including breaches of employment contract obligations, thus extending civil and employment law obligations into the area of criminal law.

The BRAK concluded that the Commission's proposal goes beyond the objective of creating a harmonized criminal law on corruption, which is commendable in itself, having "overshot the mark" in terms of content and function. The DAV summed up that the proposal is not in line with the *ultima-ratio* principle of criminal law and provides for an apodictic increase of penalties without regard to internal coherence. (TW)

### First Meeting of EU Network against Corruption

On 20 September 2023, the EU network against corruption met for the first time. The network was established by the Joint Communication on combating corruption that was drafted by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy and presented on 3 May 2023 (→eucrim news supra). The aim is to foster collaboration, identify trends and maximise the impact and coherence of European efforts to prevent and fight corruption in order to create more effective anti-corruption policies.

The network is meant as an umbrella forum for all stakeholders in the EU to exchange good practices, and brainstorm ideas and plans for further work. Participants of the first meeting *inter alia* discussed the following topics:

- Objectives and potential added value of the network;
- Good practices and trends identified in the 2023 Rule of Law report, such as fight against corruption in seaports, use of technology for prevention and repression of corruption, and education and awareness-raising;
- Issues for future investigation.

The Commission presented the most relevant funding opportunities for anti-corruption projects under Erasmus+, the Internal Security Fund (ISF), and the Technical Support Instrument (TSI). For 2024, one of the main tasks of the network will be to map high-risk areas for corruption. The work of the network will also feed into the planned comprehensive EU strategy against corruption. (TW)

### Commission Formally Closes Cooperation and Verification Mechanism for Bulgaria and Romania

On 15 September 2023, the European Commission formally closed the Cooperation and Verification Mechanism (CVM) for Bulgaria and Romania. The closure comes after the Commission formally consulted the Council and the European Parliament in July 2023.

The CVM was established upon accession of Romania and Bulgaria to the EU in 2007 in order to remedy certain shortcomings that existed in both countries, in the areas of judicial reform and the fight against corruption, and, concerning Bulgaria, the fight against organised crime. These weaknesses were thought to prevent an effective application of EU laws, policies, and programmes. The Commission regularly verified the countries' progress against specific benchmarks, which were included in the CVM.

The Commission ended the CVM because all benchmarks had been satisfactorily met. This was already concluded in the last progress reports for both Member States (→eucrim 4/2022, 243).

Monitoring of the countries continues by means of the EU's "Rule of Law toolbox" which applies to all EU Member States. It includes both preventive tools with the Rule of Law Cycle and annual reports with recommendations, as well as reactive tools such as infringement procedures or the conditionality regulation. In addition, Member States must fulfill certain

milestones for their judiciary and anti-corruption frameworks in order to obtain financial means from the Recovery and Resilience Facility (RRF). (TW)

### Council Calls to Increase Efforts to Tackle Corruption

On 4 May 2023, the Council adopted conclusions on corruption as an obstacle to development. The conclusions emphasise the increased urgency of adopting a whole-of-government approach to combatting corruption in context of the COVID-19 pandemic and the illegal war of Russia against Ukraine. In particular, the Council highlights the importance of the following points:

The Commission and the EEAS are invited to provide regular updates on the progress made in reducing corruption across the EU. This should involve ensuring that the existing reporting mechanisms accurately capture all EU measures aimed at combating corruption in a comprehensive manner. (SH)

### ECJ Rules on Automatic Penalties for Conflict-of-Interest Situations in Leading Administrative Positions

EU law does not preclude a person from being prohibited from all elective public office for three years if he/she has infringed the rules relating to conflicts of interest by holding such office. This statement was made by the ECJ in its judgement of 4 May 2023 in Case C-40/21 (*T.A.C. and Agenția Națională de Integritate (ANI)*). The case concerned Romanian legislation on administrative law.

➤ *Background of the case and legal question*

In 2016, the person concerned involved in the Romanian legal case was elected mayor of a municipality in Romania for a four-year period. Subsequently, in 2019, the *Agenția Națională de Integritate* (National Integrity Agency, Romania) conducted an investigation and concluded in a report that the mayor had failed to comply with the rules governing conflicts of interest in administrative affairs. This report would have the effect that his term as mayor would automatically come to an end, and he would face an additional three-year ban on holding any elective public office.

The mayor filed a lawsuit seeking to invalidate the report, claiming that EU law precludes automatic penalties without the possibility of modulation for those in conflict-of-interest situations. The referring Romanian court inquired with the ECJ about the compatibility of the prohibition under Romanian law with the principle of proportionality of penalties, the right to engage in work, and the right to an effective remedy and access to an independent tribunal, all of which are safeguarded by the Charter of Fundamental Rights of the European Union (CFR).

➤ *The ECJ's ruling*

➤ *Does the principle of proportionality of penalties (Art. 49(3) CFR) apply to measures imposed pursuant to an administrative procedure?*

The ECJ continued its case law from "Ecotex Bulgaria" (C-544/19) and held that Art. 49(3) CFR only applies if the prohibition was criminal in nature. This should be determined on the basis of three criteria: first, the legal classification of the offence under national law; second, the intrinsic nature of the offence; and third, the degree of severity of the penalty which the person concerned is liable to incur.

The Court emphasized that, although the prohibition in question (Art. 25(1) and (2) of Law No 176/2010) is not classified as criminal law by Romanian law, the intrinsic nature of the offence in question and the degree of severity of the penalties to which it is liable to give rise may nevertheless result in its being criminal in nature.

However, the Court found that, given first, the prohibition was issued on the basis of an administrative procedure and second, the prohibition did not pursue a repressive objective (as the focus was on preserving the integrity and function of the Romanian state), the intrinsic nature of the prohibition is not criminal in nature. Furthermore, several factors, such as the limited duration of the ban, a limited target group of persons, and the measure not imposing a sentence of deprivation of liberty or a fine as well as not applying to the right to vote, do not fulfill the third criterion either. As a result, none of the three criteria was fulfilled, the prohibition was not of a criminal nature and the scope of application of Art. 49(3) of the Charter was not opened.

➤ *Does the principle of proportionality preclude measures prohibiting the holding of any elective public office for a predetermined period of three years?*

The judges in Luxembourg stressed that, although Art. 49(3) CFR is not applicable, in any event, the principle of proportionality, as a general principle of EU law must be considered. In this regard, the measure must be suitable for securing the attainment of the legitimate objective pursued and not go beyond what is appropriate and necessary in order to attain it.

Regarding the suitability, they state that the automatic disqualification from office ends the conflict of interest with immediate effect. The imposition of the ban from office secures this for the next three years. Consequently, the regulation is suitable for achieving its objectives.

Furthermore, they found that the measure is necessary because of the serious implications of a conflict of interest in a public elective office. In addition, the provision is to be attributed to the effort to comply with a decision of the Commission of the EU (2006/928/EC) that addresses specific benchmarks for the Romanian state in the fight against corruption.

As to appropriateness, the judges in Luxembourg decided that the public in-

terest in a corruption-free administration, in principle, outweighs the penalty, especially in the national context of increased risk of corruption. However, in individual cases, the rigid penalty of a three-year ban from office without the possibility of modulation could be disproportionately high. This is a matter for the referring Romanian court to decide, taking into account all the details of the case.

➤ *Does the right to engage in work, the right to an effective remedy and to a fair trial preclude the infringed Romanian law?*

The right to engage in work and to pursue a freely chosen or accepted occupation is enshrined in Art. 15(1) CFR. The ECJ found that, although the fundamental right has a broad scope, it does not include the right to hold a democratically obtained electoral mandate for a specified period of time. Special legal provisions in Title V of the Charter entitled "Citizens rights" justify this conclusion.

Regarding the guarantees enshrined in Art. 47 CFR, the ECJ stressed that the person concerned has had an effective opportunity to challenge the legality of the report that made the finding of a conflict of interest and the penalty imposed on the basis of it, including its proportionality. According to the ECJ, Romanian law seems to respect these parameters: The court in Romania is independent and has the power to overrule the National Integrity Agency's evaluation report in which the mayors' conflict of interest was established. (SH)

## Money Laundering

### New Rules for Crypto-Assets in the EU

At the end of May 2023, the EU passed new legislation with regard to crypto-assets. The new legislation is designed to prevent misuse of the crypto industry for the purposes of money laundering and financing of terrorism as follows:

- In order to make it more difficult for criminals to circumvent anti-money laundering rules via crypto currencies, the European Parliament and the Council established Regulation 2023/1113 on information accompanying the transfers of funds. The regulation overhauls and extends the scope of Regulation 2015/847 with regard to transfers of crypto-assets, the objective being to ensure financial transparency and to provide the EU with a robust framework for the exchange of crypto-assets – in line with international standards. Crypto-asset service providers will be required to collect and make available information about the sender and beneficiary of transfers of crypto-assets, regardless of the amount of crypto-assets transacted. The new Regulation will apply from 30 December 2024.
- The European Parliament and the Council also adopted new rules on markets in crypto-assets (MiCA). The MiCA proposal was first presented on 24 September 2020 and is part of the EU's wider digital finance package, which aims to develop a European approach that promotes technological development and ensures financial stability and consumer protection. The MiCA Regulation (Regulation 2023/1114) intends to protect investors and preserve financial stability, while fostering innovation and promoting the attractiveness of the crypto-asset sector. MiCA will also protect consumers from some of the risks associated with investing in crypto-assets. For example, by imposing stricter requirements on crypto-asset service providers and making them liable should they lose investors' crypto-assets, the regulation will help consumers avoid fraudulent schemes. Stablecoin issuers will be required to build up a sufficiently liquid reserve, at a ratio of 1:1 and partly in the form of deposits. Overall, stablecoins will be supervised by the European Banking Authority (EBA), with the issuer's presence in the EU being a prerequisite for any issuance. Non-fungible tokens (NFTs) will be excluded from the scope of MiCA, unless they fall under existing categories for crypto-assets. The MiCA Regulation also applies from 30 December 2024. By way of derogation, several provisions apply earlier. (AP)

### 2022 EBA Review: Progress in the Fight Against ML/TF

On 11 July 2023, the European Banking Authority (EBA) published findings from the review it conducted in 2022 on how competent authorities are addressing money laundering and terrorist financing (ML/TF) risks in the banking sector. The EBA regularly conducts these reviews on the basis of its legal mandate to ensure effective and consistent supervisory practices, to contribute to the application of Union law, and to prevent misuse of the EU's financial system for ML/TF. The findings and recommendations of the report are relevant for all competent authorities supervising ML/TF risks in credit and financial institutions across the EU. This is now the third report on competent authorities' approaches to the supervision of banks with respect to AML and CFT (for the 2022 report →eucrim 1/2022, 26–27; for the first report →eucrim 1/2020, 16).

Overall, the EBA found that progress has been made in the fight against ML/TF, with some authorities making significant changes that have led to more effective AML/CFT supervision of banks. While many competent authorities have made tangible progress in addressing ML/TF risks through prudential supervision and improved cooperation and information sharing, challenges remain in the assessment of ML/TF risks and a lack of formalised processes and targeted training for AML/CFT and prudential supervisors, sometimes leading to missed opportunities for early intervention.

This is why the EBA has now provided guidance to competent authorities on steps to strengthen their approach.

The EBA is currently in its fourth and final round of implementation reviews of competent authorities. A final report will be published assessing the progress made since 2019. (AP)

### AML: Commission Updated List of High-Risk Third Countries

Under Directive (EU) 2015/849, the European Commission is responsible for identifying high-risk third countries with strategic deficiencies in their anti-money laundering and counter-financing of terrorism (AML/CFT) regimes. As set out in Art. 18a, this Directive requires banks and other financial institutions to exercise heightened vigilance when dealing with such high-risk third countries. The identification and listing of third countries whose AML/CFT regimes have strategic deficiencies aims to protect the integrity of the EU's financial system and internal market, reinforce internal security and promote sustainable development.

The Commission regularly updates the list of high-risk third-country jurisdictions, which takes the legal form of a delegated regulation (→eucrim 2/2020, 89). It enters into force after scrutiny and non-objection by the European Parliament and the Council over a period of one month (which can be prolonged for another month). In May and and August 2023 the Commission adopted new Delegated Regulations pertaining to high-risk third countries. They were published in the Official Journal (L series) of 26 June 2023 and 28 September 2023, respectively.

The update of May 2023 added Nigeria and South Africa as third-country jurisdictions with strategic deficiencies in their AML/CFT regimes, while two other jurisdictions were delisted: Cambodia and Morocco. The update of August 2023 blacklisted Cameroon and Vietnam.

The Commission's assessment of high-risk third countries is based on a revised methodology adopted in May 2020 (→eucrim 2/2020, 89). In total, the Commission identified 132 jurisdictions so far that will be further analyzed according to its methodology over the period 2018–2025. As a matter of priority, a first group of 54 jurisdictions (Priority 1 countries) is reviewed and constantly reassessed when new relevant information sources become available. The other jurisdictions (Priority 2 countries) will be assessed successively until 2025. It is important to note that the Commission takes into account the list of "jurisdictions under increased monitoring" made up by the Financial Action Task Force (FATF), but the Commission assesses the countries and drafts the EU list autonomously. (AP/TW)

### First High-Level Expert Meeting on Money Laundering and Asset Recovery

On 19 and 20 June 2023, Eurojust organised the first high-level expert meeting on money laundering and asset recovery. It was attended by specialised prosecutors from the EU and from countries with liaison prosecutors at Eurojust as well as by representatives of the European Commission, other EU agencies and bodies, the Financial Action Task Force, and the CARIN Network. Representatives from Interpol and other law enforcement agencies also attended, together with experts in cryptocurrencies and representatives of Financial Intelligence Units and the Egmont Group. As an outcome of the meeting, the experts expressed their support for setting up a dedicated Focus Group on Money Laundering and Asset Recovery in order to increase national and cross-border inter-institutional cooperation between the judiciary, law enforcement, and other actors involved in the fight against money laundering and for the recovery of criminal assets. (CR)

## Tax Evasion

### EP Resolution on Lessons from the Pandora Papers

In a resolution on lessons learnt from the Pandora Papers and other revelations, adopted on 15 June 2023, the European Parliament (EP) made a number of recommendations stemming from data leaks on tax evasion and money launderings schemes, such as the Pandora Papers. The resolution addresses the protection of journalists and whistle-blowers, the reduction of conflicts of interest, better regulation of intermediaries, improvements in reporting and information sharing (particularly on beneficial ownership), efforts against harmful tax practices, and measures against the misuse of shell companies and opaque structures.

The MEPs stressed the role of journalists and whistleblowers in investigating and exposing potential violations of tax law as well as corruption, organised crime, and money laundering. In order to better protect from SLAPPs (strategic lawsuits against public participation) those persons who engage in public participation, the MEPs backed the Commission's proposal for an anti-SLAPP directive (→eucrim 2/2022, 119) and called on Member States to adopt said legislation. The EP expressed dismay over the fact that 24 Member States failed to transpose and communicate the transposition of the Whistleblower Directive within the deadline and welcomed infringement procedures initiated by the Commission against at least 19 Member States for their failure to transpose it (→eucrim 2/2022, 118).

The MEPs distanced themselves from a number of EU high-level decision-makers mentioned in the Pandora Papers. They stressed that, due to importance of safeguarding the high standards of integrity, honesty, and responsibility among public officials

in the EU and in the Member States as well as fostering, within that environment, a sense of duty and personal honesty, Members of the European Parliament must honourably disclose any "financial interests which might influence the performance of the Member's duties."

Regarding the role of intermediaries in facilitating tax evasion and avoidance, the EP pointed out that the Pandora Papers exposed PwC and other major accountancy firms for their central role in assisting Russian oligarchs' investments in the West through the firms' networks of offshore shell companies. In light of these revelations, the MEPs called on the Commission and the Member States to further analyse and address potential conflicts of interest stemming from the provision of legal advice, tax advice, and auditing services when advising both corporate clients and public authorities.

The MEPs further stressed the need for new, appropriate, and targeted regulations on new technologies (e.g. crypto-assets), which present challenges in the area of tax avoidance and money laundering. Furthermore, they expressed concerns over schemes granting nationality or residency on the basis of financial investment, also known as "golden passports". The resolution calls on the Commission to report on progress made by Member States in repealing or withdrawing the citizenship or residence permits of Russian or Belarusian individuals who have obtained their status through investment.

In the fight against tax evasion/avoidance, the Commission is invited to assess feasibility of legislation to establish mechanisms for unexplained wealth at the EU level. Regretting the lack of transparency on the part of the Commission and the Member States regarding the progress made in freezing and seizing the assets of sanctioned persons, the resolution also called on the Commission to publish a list of assets that have been frozen or confiscated following Russia's invasion of Ukraine. The MEPs expressed support for the Commission 2022 proposal on asset recovery and confiscation (→eucrim 2/2022, 76). The MEPs blamed the Council's lack of willingness to agree on the forthcoming transparency criterion with regard to ultimate beneficial ownership. Concealment thereof was a common feature in the schemes exposed by the Panama Papers and a key contributing factor to the continuation and success of such schemes.

Lastly, the EP called for greater transparency concerning preferential tax systems and more tax solidarity among EU Member States.

The resolution is based on a report authored by *Niels Fuglsang* (S&D, DK) and adopted by the EP's Committee on Economic and Monetary Affairs at the end of March 2023. The findings and recommendations follow up several hearings in the EP and country visits by EP delegations after a number of data leaks on tax evasion schemes in recent years. The EP has addressed the challenges unveiled by the Pandora Papers and other similar leaks by assessing different policy areas. (AP)

## Counterfeiting & Piracy

### Almost 900,000 Counterfeit Products Seized in Anti-Smuggling Operation

At the beginning of May 2023, a major anti-smuggling operation (Operation Pirates 1) was carried out by 15 EU Member States and Frontex with the support of Europol, OLAF, the European Union Intellectual Property Office (EUIPO), the Customs Eastern and South-Eastern Land Border Expert Team (CELBET), the Law Enforcement Working Party Customs Cooperation (LEWP-C), and the Pharmaceutical Security Institute (PSI). Operation Pilates 1 led to the seizure of 810,995 counterfeit products and 61,246 counterfeit electronic devices, with the total amount of all seized goods exceeding €33 million. The seizure included clothes infringing the rights of more than 60 trademarks, footwear, and accessoires like bags, wallets, belts, sunglasses, etc. as well as perfumes, electric bikes, and watches.

Counterfeit products not only undermine the legitimate market and the EU budget but also pose a danger to the health of the consumers. The operation was part of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) – a recurring four-year cycle to identify, prioritise, and address threats posed by organised and serious international crime. (CR)

## Organised Crime

### IOCTA 2023

On 17 July 2023, Europol's European Cybercrime Centre (EC3) published the ninth edition of its Internet Organised Crime Threat Assessment (IOCTA) 2023. The IOCTA is a strategic analysis report providing an assessment of the latest online threats and the impact of cybercrime within the EU from a law enforcement point of view.

The 2023 edition presents the main overall findings concerning the different typologies of cybercrime, namely cyber-attacks, online fraud schemes, and online child sexual exploitation. It is accompanied by a series of in-depth articles covering each of these crime areas. The 2023 IOCTA also looks at online criminal markets: the surface web and the Darknet. It additionally addresses the convergence of cyber and terrorism.

In 2022, Russia's invasion of Ukraine resulted in a boost in cyber-attacks worldwide. Online fraudsters also swiftly adapted to the new geopolitical situation by exploiting the crisis. Looking at the criminal profits, the report identifies money mules as key facilitators for the laundering of illicit

profits generated by cybercrime. As regards the threat of online child sexual exploitation, the report registers a further increase in terms of quantity and severity. The following are the key findings of the report:

- Cybercriminal services are intertwined and their efficacy is co-dependant;
- Human oversight is the weakest link by which cybercriminals infiltrate their victims' systems;
- The central commodity of this illicit economy is stolen data;
- Cybercrime is often interlinked, presenting a concentrated set of criminal actions that often result in the same victim being targeted multiple times;
- Underground communities educate and recruit cybercriminals.

In addition to the report, a series of spotlight reports examining specific crime areas relating to cybercrime will be released by Europol in the course of 2023. Focus will be on cyber-attacks, online fraud, and child sexual exploitation. (CR)

### Terrorism

#### Europol TE-SAT 2023

On 14 June 2023, Europol published its EU Terrorism Situation and Trend Report (TE-SAT) 2023. The report was updated at the request of the Member States on 26 October 2023. It gives an overview of terrorism in Europe in 2022, analyses the situation regarding Jihadist, right-wing/left-wing and anarchist terrorism, ethno-nationalist and separatist terrorism as well as other forms of terrorism and extremism. It also provides an outlook on potential developments.

The year 2022 saw a total of 28 completed, failed, and foiled terrorist attacks recorded in the EU compared to 15 attacks in 2021. EU law enforcement authorities arrested 380 suspects for terrorism-related offences (compared to 388 in 2021), and 427 verdicts (convictions and acquittals) for terrorist offences were passed by courts in the Member States.

Two Jihadist terrorist attacks were carried out by individuals acting alone. While no failed attacks were reported, four jihadist attacks were foiled in six EU Member States, and 266 suspected Jihadists arrested in 2022.

In the area of right-wing terrorism, one right-wing terrorist attack was completed in 2022. No failed attack was reported, three attacks were foiled, and 45 arrests of right-wing terrorists were made in nine EU Member States.

In the field of left-wing terrorism, 13 left-wing terrorist attacks were completed and carried out in 2022 compared to one attack in 2021. The majority of the attacks (8) took place in Italy.

No completed, failed, or foiled attack was carried out by ethno-nationalist and separatist terrorists in the EU in 2022. 18 individuals were arrested for involvement in ethno-nationalist and separatist activities in four EU Member States.

Looking at potential developments in terrorism and violent extremism in the EU, the report sees the lines between different types of terrorism becoming increasingly blurred in the future. In addition, right-wing, left-wing, and environmentally inspired terrorism and violent extremism are expected to gain further prominence. Geopolitical developments outside the EU will continue to have an impact on terrorism and violent extremism within the EU. While lone actors are expected to continue to perpetrate most of the terrorist attacks in the EU, terrorist organisations may exploit the increasing fluidity of the radicalisation processes taking place – especially in the online environment. The online environment and emerging technologies will regrettably be key in enabling propaganda, recruitment, and the coordination of terrorist and violent extremist activities. According to the report, there is also reason to fear that terrorists may display increasing interest in technologically enhanced or enabled weaponry in the future. (CR)

## Procedural Law

### Procedural Safeguards

#### ECJ: National Prohibitions to Examine Violations of the Duty to Inform Suspects of their Right to Remain Silent Possible

EU law does not preclude national legislation which prohibits the trial court in a criminal case from raising of its own motion a breach of the obligation imposed on the competent authorities to inform suspects or accused persons promptly of their right to remain silent with a view to the annulment of the procedure. However, those suspects or accused persons must not have been deprived of a practical and effective opportunity to have access to a lawyer. On 22 June 2023, this reply was given by the ECJ to a reference for preliminary ruling from the *tribunal correctionnel de Villefranche-sur-Saône* (Criminal Court, Villefranche-sur-Saône, France). The case is referred to as C660/21 (*Procureur de la République v K.B. and F.S.*).

➤ *Background of the case*

On 22 March 2021, two individuals were arrested by police officers whilst stealing fuel. During the criminal proceedings brought against them, the court found that certain investigative acts and self-incriminating statements were taken from them before they were informed of their rights, including the right to remain silent, which is in violation of the national law transposing Arts. 3 and 4 of Directive 2012/13.

Due to the delay in informing them of their rights, the Criminal Court, Villefranche-sur-Saône, ruled that their right not to incriminate themselves had been violated. As a consequence,

the court considered annulling the vehicle search, the suspects' detention in custody, and all the related acts. However, in French criminal law, pleas of procedural invalidity, such as the breach of the right to be informed of the right to remain silent when placed in custody, must be raised by the individuals or their lawyer before presenting any defense on the merits. Neither the suspects nor their lawyer had raised such a plea before their defense in the case at hand.

The referring court sought guidance from the ECJ on whether the prohibition of French courts raising, on their own motion, a breach of the obligation to inform suspects and accused persons promptly of their right to remain silent, is compatible with EU law.

➤ *The ECJ's ruling*

The Court recalled that the right to remain silent is safeguarded not only by Art. 48 CFR, relating to the presumption of innocence and right of defense, but also by Art. 47(2) CFR, relating to the right to a fair hearing. Directive 2012/13/EU is based on the mentioned fundamental rights guarantees and imposes an obligation on Member States to inform suspects or accused persons promptly of their rights, including the right to remain silent, before the first official interview with the police or another competent authority.

The ECJ emphasized that, when implementing the Directive, Member States must ensure that the right to an effective remedy and a fair hearing, as laid down in the Charter, are respected. Besides this, Member States have some leeway to establish that procedure. The Court found that, if suspects have practically and effectively had the right of access to a lawyer, if necessary having obtained legal aid, have had a right of access to their file and the right to invoke that breach within a reasonable period of time, national provisions for courts in a criminal case to challenge breaches are within this leeway. Therefore, it is possible to limit the time within which such a breach may be invoked. Moreover, if the suspect or his/her lawyer waive that opportunity, they must bear the possible consequences of that waiver.

The ECJ concluded that national prohibitions, such as the French one in question, do not violate Directive 2012/13 as well as Arts. 47(2) and 48 CFR, but left open the question whether there had been a procedural shortcoming. This is a matter falling to the domestic courts to assess. In consequence, French courts are still prevented from raising of their own motion a breach of the obligation to inform suspects promptly of their right to remain silent after the presentation of a defense on the merits. (SH)

### ECJ Clarifies Rights of Suspects in the Event of Personal Search and Seizure

On 7 September 2023, the ECJ ruled on the scope of Directives 2012/13 on the right to information in criminal proceedings and (EU) 2013/48 on the right of access to a lawyer in criminal proceedings when persons are subjected to a strip search for drug possession and the seizure of illegal substances or assets. The case at issue concerned Bulgarian criminal procedure law and practice (Case C-209/22, *AB v Rayonna prokuratura Lovech*).

➤ *Background of the case*

In the main proceedings, the referring District Court of Lukovit (Bulgaria) had to rule on the approval of these measures, which Bulgarian police officers carried out against AB following a vehicle check. The referring court had doubts as to the compatibility of Bulgarian criminal procedure law with the aforementioned directives. First, under Bulgarian law, the rights under the directives are granted only to "accused persons" and not to "suspects", so that in police and prosecutorial practice the obligations to safeguard the rights of the defense are generally not complied with until the person concerned is not formally regarded as an "accused person". Secondly, the Bulgarian courts' right of review in pre-trial proceedings is limited to formal legality; a violation of Arts. 47 and 48 of the Charter and the rights guaranteed in the directives cannot be examined here according to Bulgarian case law. If Bulgarian law violates EU law, the question arises for the referring court as to what consequences it can draw from this for its decision in the preliminary investigation proceedings.

➤ *ECJ's decision on the applicability of the Directives*

In a first step, the ECJ affirms the applicability of the two Directives 2012/13 and 2013/48 to the present case. The scope of application coincides and presupposes that two elements are required: (1) Suspicion on the part of the competent authorities that the person concerned has committed a criminal offence and (2) information in this regard is provided to the person by "official notification or otherwise". The ECJ considers the conduct of the strip search and seizure to be based not only on the fact that the person has been suspected of a criminal offence, but also that the person concerned has been implicitly informed of the suspicion of a criminal offense. The requirements for the application of the directives are therefore fulfilled. The fact that national law does not recognise the concept of "suspect" and that that person has not been officially informed that he or she is an "accused person" is irrelevant in that regard.

➤ *Requirements for judicial review*

With regard to the question of the limited scope of review, the judges in Luxembourg point out that the directives grant the Member States a certain margin of discretion to determine the specific procedures with regard to the modalities and timing of asserting violations of rights. The legal remedy must merely be effective. The Member States are not obliged to cre-

ate new legal remedies (unless no legal remedy exists that would make it possible to ensure, even indirectly, respect for the rights that individuals derive from EU law).

Accordingly, EU law does not preclude national case law according to which the court that, under the applicable national law, is seized of an application for *ex post* authorization of a strip search and the resulting seizure of illegal substances, carried out in the course of the preliminary stage of criminal proceedings, is not empowered to examine whether the rights of the suspect or accused person guaranteed by those directives have been respected. However, that person must subsequently be able to have any infringement of the rights under those directives established before the criminal court and that court must then be obliged to draw conclusions from such infringements, in particular with regard to the inadmissibility or probative value of the evidence obtained in those circumstances.

➤ *Access to a lawyer*

Lastly, the ECJ addresses the question of whether legal counsel should have been present during the strip search and seizure of illegal goods in accordance with the obligations under the Directive. The ECJ concludes from the principle rules in Art. 3(2) and Art. 3(3) of Directive 2013/48 that the strip search and seizure, which in the present case also occurred as a result of a roadside check, are not actually contexts in which the person concerned could have had the right of access to a lawyer. However, the Bulgarian court had to examine whether the presence of a lawyer was objectively necessary for the suspect to be able to exercise his defense rights practically and effectively.

➤ *Put in focus*

The ECJ has had to decide several times on the compatibility of Bulgarian criminal procedure law with the guarantees enshrined in the EU's procedural rights directives. In May 2023, the ECJ already had to deal with the missing concept of "suspect" under Bulgarian law and indicated that procedural rules on information to detained persons are incompatible with Directive 2012/13 (→next news item). In this judgment, the ECJ made clarifications on the applicability of the Directives as well. As in the present judgment, the ECJ emphasised that national authorities cannot circumvent the obligations deriving from the procedural rights directives if they do not formally recognise a person as suspect or "accused person". In essence, this line of argument strengthens the position of persons suspected of a criminal offence to be informed of their procedural rights and to have access to a lawyer at the earliest stages of criminal proceedings.

In November 2021, the ECJ ruled that Bulgaria cannot issue European Investigation Orders as long as it does not provide for legal remedies against coercive investigative measures (→eucrim 4/2021, 228–229). (TW)

### ECJ: Information on the Detention Grounds Must Be Prompt and Specific

In a judgment of 25 May 2023, the ECJ clarified the applicability of Directive 2012/13 on the right to information in criminal proceedings as well as the modalities, timing and the level of detail of information, which must be given to suspects.

➤ *Facts of the case and questions referred*

The case (C-608/21, *XN v Politseyski organ pri 02 RU SDVR*) is based on questions referred by the Sofia District Court (Bulgaria), which had to examine the legality of a police detention order on suspicion of "disturbance of public order" against the plaintiff (XN). XN participated in protests and was detained by police officers from the Bulgarian Ministry of Interior. As grounds for detention, the police officers merely referred to "Article 72(1) of the Law on the Ministry of the Interior" and "disturbance of public order". Other written police reports were only submitted at a later stage in the criminal proceedings. The referring court pointed out that the detention constituted an administrative coercive measure with the purpose of preventing the person concerned from absconding or committing an offence. Furthermore, the Supreme Administrative Court of Bulgaria considers permissible to provide information of factual and legal grounds for this detention in accompanying documents drawn up beforehand or afterwards, and it is seen sufficient to provide these information in the event the person concerned challenges the legality of the detention before courts. The referring court had doubts as to whether the Bulgarian legislation and case law is in line with Directive 2012/13, in particular its Art. 6(2) and asked:

- Is it permissible that information concerning the grounds for detaining a suspect, including information concerning the criminal offence of which he/she is suspected, is not contained in the written detention order, but in other accompanying documents (originating before or after that order) and which are not provided to him/her immediately?
- Which details must the information to the detained person contain?

➤ *ECJ's ruling on the applicability of Directive 2012/13 to the administrative coercive measure*

The judges in Luxembourg first clarified that, even though the detention is considered an individual administrative act under Bulgarian law, the plaintiff was suspected of a criminal offence and he was informed as a criminal suspect. Therefore, Directive 2012/13 is applicable in the present case, the requirements of its Art. 2(1) are met.

➤ *ECJ's reply to the first question referred*

The ECJ concedes that Art. 6(2) of Directive 2012/13, according to which arrested or detained persons must be informed of the reasons for their arrest or detention, including the criminal act they are suspected or accused of having committed, does neither indicate the timing nor the modalities of the information. However, Art. 6(2) must be read in the context of Art. 6(1), which lays down a general obligation to provide information on the criminal act, and the objective pursued by the Directive, which is to enable persons suspected or accused of a criminal offence to prepare their defence and to safeguard the fairness of the proceedings. These persons must be able to obtain a review of the detention or to apply for provisional release in an effective manner. Against this background, grounds for the detention of suspected/accused persons bay be set out in documents other than the detention order, however, such information must be given "promptly", i.e., at the time of the deprivation of liberty or within a short period after it has begun. It is insufficient if the information is given, as in the present case, only during an appeal that challenged the lawfulness of detention.

➤ *ECJ's reply to the second question referred*

With regard to the further question on the required detail of information, the ECJ points to the need to take account of the stage of the proceedings in the individual case. In order to guarantee the rights of the defense, in particular the right to effectively challenge detention, the relevant information must include a description of the relevant facts known to the competent authorities (time, place and nature of the person's actual participation in the alleged offence) as well as the legal classification provisionally adopted. It must also be ensured that the person concerned understands the reasons for his/her arrest or detention and is able to effectively challenge the lawfulness of that arrest or detention.

The ECJ also doubts whether the Bulgarian legislation is in line with EU law since it conferred the rights to information under Art. 6(2) of the Directive only to persons with the status of "accused person" and not to "suspects".

➤ *Put in focus*

The ECJ made an important clarification that the Directives guaranteeing procedural safeguards in criminal proceedings apply irrespective of the definition of a measure restricting a person's liberty in national law (here: detention seen as an *administrative* measure under Bulgarian law). In addition, the judges in Luxembourg clarified the objective of the Directive on the right to information in criminal proceedings, which is to guarantee the effective use of defence rights against national law enforcement. It was less a problem that all necessary information to exercise these rights effectively were not contained in the written detention order, but rather that the information was not given promptly to the detained person. (TW)

## Data Protection

### ECJ: No Use of Data Retained for Criminal Proceedings in Administrative Proceedings for Corruption

The ECJ ruled on 7 September 2023, in Case C-162/22, that retained data provided to authorities for the purpose of combating serious crime cannot be used in the context of investigations for a disciplinary offense related to corruption.

➤ *Facts of the case and question referred*

The case at issue raised the question as to whether data retained and provided by telecommunication service providers to law enforcement authorities in the context of combating serious crimes can be used in other (disciplinary) proceedings involving the misconduct of office related to acts of corruption. This is foreseen under the Lithuanian law. Concretely, a Lithuanian prosecutor is alleged to have unlawfully provided relevant information to the suspect and his lawyer in the course of investigations conducted by him. Internal investigations by the Prosecutor General's Office of the Republic of Lithuania found misconduct on the part of the prosecutor, dismissed him from his position and removed him from office. The Prosecutor General hereby relied on the information obtained from the court-ordered interception and recording of traffic and location data transmitted via electronic communications networks at the suspect's lawyer and the prosecutor subject to the proceedings of misconduct of office (main proceedings).

The referring Supreme Administrative Court of Lithuania *(Lietuvos vyriausiasis administracinis teismas)* observed that, according to the ECJ's case law on data retention, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with Arts. 7 and 8 CFR in connection with Art. 15(1) of Directive 2002/58. However, the Court has not yet ruled on the impact of the subsequent use of the data concerned on the interference with fundamental rights. The referring court sought guidance as to which extent the data retained and provided for the purpose of combating serious crime can be used in the investigations related to the misconduct in office.

➤ *The ECJ's ruling*

The ECJ reiterated its case law as to legislative measures that allow exceptions from the obligation to ensure confidentiality of personal data in accordance with Art. 15(1) of Directive 2002/58 (cf. Joined Cases C-793/19

and C-794/19, *SpaceNet and Telekom Deutschland* →eucrim 3/2022, 188–189). It also clarified that the principles developed in previous cases on data retention (cf. Case C-140/20, *G.D. v The Commissioner of An Garda Síochána* →eucrim 2/2022, 115) also apply *mutatis mutandis* to the subsequent use of traffic and location data retained by providers of electronic communications services, in detail:

- A legislative measure must correspond, genuinely and strictly, to one of the objectives exhaustively listed in Art. 15(1) of Directive 2002/58;
- There is a hierarchy amongst those objectives according to their respective importance and the importance of the objective pursued by a legislative measure must be proportionate to the seriousness of the interference that it entails;
- As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights;
- Access to traffic and location data may, in principle, be justified only by the public interest objective for which those providers were ordered to retain those data.

As a consequence, the ECJ concluded: "… data [that have been once retained and made available to the competent authorities for the purpose of combating serious crime] cannot be transmitted to other authorities and used in order to achieve objectives, such as, in the present case, combating corruption-related misconduct in office, which are of lesser importance in the hierarchy of objectives of public interest than the objective of combating serious crime and preventing serious threats to public security. To authorise, in that situation, access to retained data and the use thereof would be contrary to that hierarchy of public interest objectives."

➤ *Put in focus*

The ECJ's ruling in Case C-162/22 shows that there are still open questions as to the limits and conditions for national legislation allowing the retention of telecommunication data and its use for law enforcement purposes within the framework defined by the ECJ, notably in *Quadrature du Net and Others* (Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* →eucrim 3/2020, 184–186). The ECJ (again) emphasises that the storage of traffic and location data involves serious interference with the fundamental rights to respect for private and family life and to the protection of personal data. The clarification of the question on the subsequent use of retained data in the Lithuanian case nonetheless triggers further questions: How is "combating serious crime" defined? How is the criterion of the "hierarchy of objectives" applied in other cases? How about the use of retained data that were at first used to maintain public security and subsequently forwarded to combat a serious crime (and vice versa)? (TW)

### AG Backs Softening of Data Retention Jurisprudence for Internet Infringements

On 28 September 2023, First Advocate General (AG) *Szpunar* confirms his viewpoint that the retention of and access to civil identity data linked to the IP address used is to be permitted if this data represents the only clue for establishing the identity of persons who have committed copyright infringements exclusively on the internet. This opinion clarifies certain aspects of a previous opinion delivered in October 2022 (→eucrim 3/2022, 190–191) in the context of the preliminary ruling in the case *La Quadrature du Net – lutte contre la contrefaçon* (C-470/21). The second opinion follows the reopening of the oral proceedings before the CJEU.

According to the AG, Union law does not prevent this, even if there is no prior control by a court or an independent administrative body. IP addresses do not make it possible to determine the civil identity of the owner of an internet access and the information about the work in question does not allow any conclusions to be drawn about the private life of the persons. This is not a departure from previous case law, but a "pragmatic development" that prevents "systemic impunity of offences committed exclusively online"; it also takes sufficient account of the conflicting interests in accordance with the principle of proportionality, the AG points out.

Thus, the AG recommends the ECJ providing a "nuanced solution" regarding the exception of the prohibition of the general and indiscriminate data retention, which has been confirmed several times by the ECJ (cf. Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* →eucrim 3/2020, 184–186 and Joined Cases C-793/19 and C-794/19, *SpaceNet and Telekom Deutschland* →eucrim 3/2022, 188–189).

The case refers to practice by the *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* (High Authority for the dissemination of works and the protection of rights on the internet – Hadopi) which requests civil identity data from electronic communications operators in order to tackle infringements of property rights on the internet. Various NGOs questioned this procedure and filed lawsuits in French courts. The case is currently one of the most important cases before the CJEU: it was referred from the Grand Chamber to the Full Court. (TW)

### AG on Identity Cards: Mandatory Collection and Storage of Fingerprints is Valid

On 29 June 2023, Advocate General (AG) *Laila Medina* expressed in her

Opinion in case C-61/22 (*Landeshauptstadt Wiesbaden*) that the mandatory collection and storage of fingerprints on identity cards is valid. In the case at issue, a German citizen applied to the city of Wiesbaden (Germany) for the issuance of a new identity card. He specifically asked for the card to be issued without the inclusion of a fingerprint image in its chip. The City of Wiesbaden refused the application on the ground, among others, that Regulation (EU) 2019/1157 sets out the obligation to include an image of the fingerprints of the holder on any identity card newly issued by the Member States – on a highly secure storage medium – as from 2 August 2021. In this context, the Administrative Court of Wiesbaden raised questions as to the compatibility of the EU Regulation in question with primary EU law and the Union's rules on data protection. In detail, the court posed three questions:

- Was Art. 21(2) TFEU, rather than Art. 77(3) of that same treaty, the appropriate basis for the adoption of Regulation 2019/1157?
- Is Regulation 2019/1157 compatible with Arts. 7 and 8 read in conjunction with Art. 52(1) of the Charter of Fundamental Rights of the European Union (CFR)?
- Is said Regulation in conformity with the obligation to carry out a data protection impact assessment under Art. 35(10) of the General Data Protection Regulation?

With regard to the first question, AG *Medina* concluded that Regulation 2019/1157 had been correctly adopted on the basis of Art. 21(2) TFEU, because the reliability and trustworthiness of these identity cards has been improved through security standards, and therefore results in the facilitation of the exercise of the right of EU citizens to move and reside freely within the Member States.

As regards the second question, the AG confirmed that the limitations introduced by Regulation 2019/1157 are in conformity with the principle of proportionality and, in particular, that they are necessary and genuinely meet objectives of general interest recognised by the European Union (in this case, the objective is to prevent the risk of falsification and document fraud). As a consequence, the Regulation is in accordance with the second sentence of Art. 52(1) CFR.

Regarding the third question, the AG believes that the European Parliament and the Council were not obliged to conduct an impact assessment during the legislative process leading to adoption of Regulation 2019/1157, as the GDPR and Regulation 2019/1157 are acts of secondary legislation that rank equally. Futhermore, the GDPR does not specify any criterion in relation to which the validity of another secondary law norm of the European Union should be assessed. In conclusion, she proposes that the ECJ reply that examination of the questions referred has not revealed any factor affecting the validity of Regulation 2019/1157. (AP)

### AG: Belgian Law Must Provide Right to an Effective Judicial Remedy against Supervisory Authority

On 15 June 2023, Advocate General *Laila Medina* presented her Opinion in case C-333/22 *(Ligue des droits humains ASBL, BA v Organe de contrôle de l'information policière)*. The case concerns the relationship between direct and indirect access to personal data held by law enforcement authorities and refers to the interpretation of Belgian law in accordance with Directive 2016/680, known as the Law Enforcement (Data Protection) Directive (LED).

In the case at issue, an individual was denied a security clearance certificate by the Belgian National Security Authority due to his past participation in demonstrations. He requested that the Belgian Supervisory Body for Police Information (OCIP) identify the controllers responsible for the data processing in order to gain access to the information about him. Without offering any other information, the OCIP simply stated that it had performed all the necessary checks. Unsatisfied with this answer, the individual – assisted by the *Ligue des droits humains* – filed an action against the OCIP before the Brussels court.

The referring Brussels Court of Appeal expressed doubts as to the compatibility of Belgian law transposing the data protection rules for police and judicial authorities as foreseen in Directive 2016/680 with Union law. It pointed out that, under Belgian law, all requests by data subjects in relation to their rights to access personal data in law enforcement contexts are to be made to the OCIP and that the OCIP need only briefly and simply inform the data subject that "the necessary verifications have been carried out." In addition, Belgian law does not foresee a judicial remedy against the OCIP.

Against this background, the Brussels Court of Appeal asked first whether Arts. 47, 8(3) CFR require provision to be made for a judicial remedy against an independent data protection supervisory authority. Second, the Brussels court questioned the compatibility of Art. 17(3) LED, which lays down the necessary information to be given to the data subject by the supervisory authority, with the fundamental rights of the Charter.

First, AG *Medina* pointed out that, with regard to the LED, a data subject who exercises his/her rights indirectly through a supervisory authority must have a judicial remedy against that authority in relation to its task of checking the lawfulness of processing. The Belgian regime, in transposing the LED, obviously derogates from the principle of direct exercise of the rights of data subjects with regard to all personal data processed by police services. Such a regime is incompat-

ible with the Directive, as it establishes a blanket exemption to the direct right of access.

Secondly, AG *Medina* reiterated that Art. 17 LED, which governs the indirect exercise of rights through a supervisory authority, is compatible with the fundamental right of personal data protection and that it offers an effective remedy to the extent that:

- The supervisory authority may, depending on the circumstances, go beyond declaring that all the necessary checks have been carried out;
- The data subject is entitled to judicial review of the measures taken and to the assessment made by the supervisory authority concerning the data subject, which are subject to the obligations of the controller.

In sum, AG *Medina* stressed that it is essential to ensure that the rights of data subjects in the field of law enforcement can be exercised effectively. (AP)

### Commission Wishes to Open Negotiations with Switzerland, Iceland and Norway on PNR Agreements

On 6 September 2023, the Commission addressed recommendations to the Council for opening negotiations with Switzerland, Iceland and Norway on concluding agreements on the transfer of Passenger Name Record (PNR) data. Switzerland, Iceland and Norway are non-EU Member States but Contracting Parties to the Schengen Convention. Agreements on the transfer and exchange of PNR data are held necessary in order to ensure internal security within the common area without internal border controls. This becomes also necessary because the three countries are not bound by the EU rules on the exchange of personal data for law enforcement purposes pursuant to Directive 2016/680. Hence, the agreements would include the data protection safeguards required by EU law and they would enable the countries to lawfully receive and process PNR data on flights operated by air carriers between the EU and them. Opening negotiations are in line with the Commission's external PNR policy, which builds on international standards and addresses global security commitments. (TW)

### Commission Puts Transatlantic Data Transfers on New Basis

**spot light**

On 10 July 2023, the European Commission adopted its adequacy decision for the transfer of personal data from the EU to US companies in the private sector. The adequacy decision is an implementing act required by Art. 45 of the General Data Protection Regulation (GDPR). It is called the EU-US Data Privacy Framework (DPF).

The Commission's adequacy decision and the DPF entered into force immediately. As a consequence, public and private entities from the European Economic Area (i.e., all the 27 EU Member States as well as Norway, Iceland, and Liechtenstein) are able to transfer personal data to companies in the US which certified their participation in the EU-US DPF.

It is the meanwhile third adequacy decision. The first two ones (the Safe Harbor framework and the Privacy Shield) were declared invalid by the CJEU (rulings in Schrems I (→eucrim 3/2015, 85) and Schrems II (→eucrim 2/2020, 98–99)). According to the Commission, the new DPF takes into account the CJEU's issues, in particular the access of personal data transferred by US authorities for criminal law enforcement and national security purposes. In over 190 recitals the Commission lays down its reasoning that the standard of data protection in the USA is essentially equivalent to the EU.

The DPF provides EU individuals whose data would be transferred to participating companies in the USA with several new safeguards, e.g., to obtain access to their data, or obtain correction/deletion of incorrect or unlawfully processed data. EU individuals will also have different redress mechanisms against US companies if their data were wrongly handled.

Regarding safeguards against the collection and use of EU citizen's' personal data by US intelligence authorities, the Commission mainly relies on the Executive Order 14086 "Enhancing Safeguards for US Signals Intelligence Activities" and the complementing Regulation on the "Data Protection Review Court" issued by the U.S. Attorney General (→eucrim 1/2023, 33). These documents provide for binding safeguards that limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security, establish enhanced oversight, and include a new independent and impartial redress mechanism. The latter consists of two layers: First, EU individuals can complain about the collection and use of their data by US intelligence authorities before the "Civil Liberties Protection Officer" (CLPO) of the US intelligence community. This person is responsible for ensuring compliance with privacy and fundamental rights. In a second step, the complainant can appeal the CLPO's decision before the newly created Data Protection Review Court (DPRC) which can act independently from the US government and take binding remedial decisions. The complainant's interests are represented by a special advocate who will be selected by the court.

At the US part, the DPF will be administered and monitored by the US Department of Commerce. The US Federal Trade Commission will be competent to enforce compliance by US companies with their obligations under the DPF. The European Commission will continuously monitor relevant developments in the USA. A

first review will take place within one year after the entry into force of the adequacy decision. Subsequently, the Commission will further decide on the periodicity of the reviews after consultation with the EU Member States and the data protection authorities.

*Statements*: The Commission's drafts of the adequacy decision were criticised in advance. Among others, the EDPB saw several shortcomings in relation to certain rights of data subjects and the EP was in favour to halt the adequacy decision (→eucrim 1/2023, 33–34).

*Max Schrems*, who won the first two ECJ judgements against the Commission's adequacy decisions in relation to the USA and who has since founded the civil rights organisation nyob, criticised that the DPF is essentially a copy of the "Privacy Shield" and a substantial reform of the US surveillance law would have been needed in order to meet the ECJ's rulings. He announced that nyob will also bring the third attempt to regulate EU-US data flows before the CJEU.

At the beginning of September 2023, French MP Philippe Latombe announced that he, too, will challgenge des DPF before the EU's General Court. He argued that the DPF includes insufficient guarantees of respect for private and family life with regard to bulk collection of personal data and he found violations against procedural rules because the DPF was notified only in English and was not published in the EU's Official Journal.

By contrast, *Věra Jourová*, Commission Vice-President for Values and Transparency, defended the new adequacy decision and said that it "will provide legal certainty for businesses and will help further consolidate the EU as a powerful player in transatlantic markets, while remaining uncompromising on respecting fundamental right of Europeans for their data to be always protected." (TW)

### EDPB Provides Guidance on "Appropriate Safeguards" Assessment under LED

On 19 September 2023, the European Data Protection Board (EDPB) adopted guidelines on the application of Art. 37 of Directive 2016/680 on the protection of personal data processed for law enforcement purposes (dubbed: Data Protection Law Enforcement Directive LED). Art. 37(1) lit. a) and b) allows the transfer of personal data of natural persons from law enforcement authorities in EU Member States to third countries or international organisations in the absence of an adequacy decision. The provision requires that "appropriate safeguards" with regard to the protection of personal data exist, which must be assessed by the competent authorities in the EU.

Against this background, the EDPB guidelines pursue various objectives:

- Providing clarity on the legal standard for appropriate safeguards;
- Being a reference for EU countries if they conclude legally binding instruments in accordance with Art. 37(1) lit. a) LED;
- Providing guidance to national data protection authorities if they are involved in negotiations on such instruments or are subsequently reviewing their implementation;
- Providing support for the data controller's accountability obligations according to Art. 37(2) and (3) LED.

The EDPB calls to mind that Art. 37 LED be applied in light of the principle that the level of data protection applicable in the EU must not be undermined by the transfer of personal data to another jurisdiction. Therefore, Art. 37 LED requires an essentially equivalent level of data protection in the recipient third country or international organisation. However, this requirement relates to the specific data transfer or category of transfers at hand and not to the entire existing legislation in the third country or international organisation.

Looking at the legally binding instrument in the meaning of Art. 37(1) lit. a) LED, the guidelines stress that all relevant rules to allow overcoming any shortcomings or limitations of the legislation of the third country or international organisation in terms of data protection should be contained. In addition, Member States should review their international agreements and bring them in line with the requirements of the LED for data transfers, where this is not yet the case.

With regard to Art. 37(1) lit. b) LED, the guidelines point out that this option should only be applied when an assessment on appropriate safeguards is based on a careful analysis of the relevant legal framework and practices in the third country/international organisation. Furthermore, it is necessary that all the details of the circumstances surrounding the data transfer are known and the competent authorities carry out a risk analysis of the information sharing with regard to fundamental rights and freedoms of the data subjects, their legitimate interests and those of other persons concerned. Any other processing operation necessitates that a competent authority be aware of and consider in a granular manner the nature, scope, context and purposes of the transfer.

The EDPB also makes statements on the data controller's accountability obligations if data transfers are based on Art. 37(1) lit. b) LED. These obligations are enhanced pursuant to Art. 37(2) and (3) LED because it is the controller alone who determines, based on its own assessment, whether appropriate safeguards exist. This involves higher risks of inconsistencies, less transparency, and less legal certainty for data subjects in comparison with transfers legally framed by adequacy decisions or legally binding instruments. Hence, competent law enforcement authorities should inform their data protection authorities in regular intervals about the catego-

ries of transfers that were carried out under Art. 37(1) lit. b) LED so that an adequate "ex post" control is ensured.

The guidelines had been made subject to public consultation. Comments from national law enforcement authorities and stakeholders may feed into a second version of the guidelines. (TW)

### EP Recommendation on Lessons Learned from Misused Spyware

On 15 June 2023, the plenary of the European Parliament adopted a recommendation that outlines reforms to curb spyware abuse. The recommendation backs the conclusions of the one-year investigations by the "Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware" (PEGA).

The PEGA Committee was set up by the EP in March 2022 (→eucrim 1/2022, 13) after it became known that the Pegasus software (developed by the Israeli cyber-arms company NSO Group) was being used in over 50 countries to surveil journalists, human rights activists, lawyers, and politicians. The Committee was mandated to investigate alleged infringement or maladministration in application of EU law in relation to the use of Pegasus and equivalent spyware surveillance software. In particular, it gathered information on the extent to which Member States or third countries are using intrusive surveillance thus violating the rights and freedoms enshrined in the Charter of Fundamental Rights of the EU.

In the final EP recommendation, appeals were made to all EU institutions and Member States. In particular, MEPs stated that the illicit use of spyware has put "democracy itself at stake". They called for credible investigations, legislative changes and better enforcement of existing rules to tackle abuse. The recommendation also contains explicit calls on Poland, Hungary, Greece, Spain and Cyprus, whose governments were involved in the misuse, to scrutinize contraventions and maladministration.

Furthermore, the EP called for strict regulations of the trade in and use of spyware and sets conditions for the Member States on the continued use of the software. In particular, the use of spyware by law enforcement should only be authorised in exceptional cases for a pre-defined purpose and a limited time. Data falling under lawyer-client privilege or belonging to politicians, doctors or the media should be sheltered from surveillance (unless there is evidence of criminal activity). In addition, the enforcement of existing legal standards must be improved and the concept of "national security" must be defined in order to avoid abusive justification of spying.

With regard to the external policy dimension, MEPs demand, *inter alia*, an in-depth review of spyware export licences, stronger enforcement of the EU's export control rules, and a joint EU-US spyware strategy.

In order to raise awareness and accountability in the EU, MEPs propose the creation of an independently run European interdisciplinary research institute (EU Tech Lab). This institute should be tasked with discovering and exposing the unlawful use of software for illicit surveillance purposes, providing accessible and free legal and technological support, performing forensic analytical research for judicial investigations and reporting regularly on the use and misuse of spyware in the EU.

The recommendation has been submitted to the European Commission with the request to initiate legislative proposals on the based of this recommendation. (TW)

### Commission Proposes Procedural Rules for GDPR Enforcement in Cross-Border Cases

The General Data Protection Regulation (GDPR) enforcement process will become more efficient for data protection authorities (DPAs) through the implementation of new rules proposed by the Commission on 4 July 2023. The proposal lays forth specific procedural guidelines for authorities in situations involving persons who have a foothold in multiple Member States. The rules also seek to increase their participation and provide clarity in the complaint submission process. Businesses' due process rights will now be clearer when a data protection authority looks into a possible GDPR violation. The new Regulation harmonises the following areas:

- Rights of complaints: By harmonising the conditions according to which a cross-border complaint can be admitted, the proposal overcomes existing barriers involving DPAs, which currently have to follow different national procedural rules;
- Rights of parties under investigation: The proposed regulation introduces the possibility for the parties under investigation to be heard at key moments in the procedure, such as during dispute resolution, by the European Data Protection Board (EDPB). It also regulates access to the administrative file's contents as well as the parties' access rights to the file.
- Streamlining cooperation and dispute resolution: Early on in investigations, DPAs shall be able to voice their opinions. The proposal offers standardised deadlines for cross-border cooperation and dispute resolution as well as specific guidelines for speeding up implementation of the GDPR's dispute resolution system.

The overall goal is to support the timely completion of investigations and the delivery of swift remedies for individuals. This proposal marks the Commission's response to the feedback received after its call for evidence from a wide variety of stakeholders, including civil society and industry associations. It addresses the input from a wide range of stakeholders: the EDPB; representatives from civil society, businesses, academia; legal practicioners;

and Member States. The incorporation of this input was also reiterated by *Didier Reynders*, Commissioner for Justice:

"[…] Today, we have come forward with this proposal to show that we can do better to have quicker and more efficient handling of cases. We have listened to the voices of the European Data Protection Board, Data Protection Authorities, civil society, and the industry. Our proposal addresses their calls and builds on our own findings to better protect Europeans' right to privacy, provide legal certainty to businesses, and streamline cooperation between data protection authorities on the ground". (AP)

## Ne bis in idem

### ECJ: Art. 50 of the Charter Protects Volkswagen from Further Administrative Penalties in Italy

spot light

The Italian competition and market supervisory authority can no longer impose an administrative fine on Volkswagen (VW) for the installation of inadmissible defeat devices in their diesel vehicles after VW had received and paid a fine from the public prosecutor's office in Germany in the meantime and in the same context. This was decided by the ECJ in Case C-27/22 on 14 September 2023, following Advocate General *Sanchez-Bodona's* opinion of 30 March 2023 (→eucrim 1/2023, 35–36).

➤ *Facts of the case*

In August 2016, the Italian competition and market authority (AGCM) imposed a fine of €5 million on Volkswagen Group Italia SpA (VWGI) and Volkswagen Aktiengesellschaft (VWAG) for unfair commercial practices against consumers. The infringements in question concerned, first, the marketing in Italy, from 2009, of diesel vehicles equipped with systems intended to distort the measurement of pollutant emissions and, second, the dissemination of advertising messages which emphasised the compliance of those vehicles with the criteria provided for under environmental legislation. VWGI and VWAG challenged the decision of the Italian competition authority before the Regional Administrative Court, Lazio, Italy.

In June 2018, before that Lazio court delivered its judgment, the public prosecutor's office of Brunswick, before which the case had been brought in Germany, imposed a fine of €1 billion on VWAG, in accordance with the Act on Regulatory Offences (*Ordnungswidrigkeitengesetz*). That fine penalised negligent breach of the duty of supervision in the activities of undertaking, in particular as regards the development of the software for the illegal defeat device and its installation in 10.7 million diesel vehicles marketed worldwide (700,000 of which were sold in Italy).

The decision of that German public prosecutor's office became final on 13 June 2018, since VWAG waived its right to challenge it and, moreover, paid the fine prescribed therein. VWGI and VWAG argued before the Italian court that they do no longer need to pay the fine imposed by AGCM because the principle *ne bis in idem* applies.

➤ *Questions raised*

The Italian Council of State (*Consiglio di Stato*), before which an appeal was brought following the dismissal of the action at first instance, asked the ECJ whether the principle *ne bis in idem* applies in the case at issue. That principle, enshrined in Art. 50 of the Charter of Fundamental Rights of the European Union, prohibits a duplication both of proceedings and of penalties of a criminal nature for the same acts and against the same person. The referring court raised three question in this regard:

- Does the fine by the AGCM, which is classified as an administrative penalty under Italian legislation, constitute a criminal penalty which would trigger Art. 50 CFR?
- Does Art. 50 CFR apply when a second decision imposed a fine criminal in nature and became final during the ongoing judicial proceedings brought against the first decision?
- May limitations of the application of the principle *ne bis in idem* be justified?

➤ *ECJ on criminal nature of administrative fines*

The judges in Luxembourg reiterate that the assessment of whether proceedings or penalties are criminal in nature rely on three criteria: (1) legal classification of the offence under national law; (2) intrinsic nature of the offence; (3) degree of severity of the penalty which the person concerned is liable to incur.

The judges in Luxembourg first clarify with regard to the first criterion that the classification under domestic law is not decisive and Art. 50 CFR also extends to proceedings and penalties that have a "criminal nature".

As regards, in particular, the second criterion, the ECJ stressed that even if the penalty at issue has also a preventive (deterrent) purpose, this does not exclude it from being classified as criminal. A further argument in favour of a classification of the administrative penalty in Italy as "criminal" is the fact that the fine varies according to the gravity and duration of the infringement in question and that it can even exceed the amount of the unfair competitive advantage.

Looking at the third criterion, the ECJ observed that the financial administrative penalty, which is capable of reaching an amount of €5 million as a maximum, has a high degree of severity.

In sum, the judges in Luxembourg affirm that the penalties imposed for unfair commercial practices can be classified as administrative penalties of a criminal nature, which makes Art. 50 CFR applicable.

➤ *ECJ on ne bis in idem conditions*

The ECJ first provides clarification regarding the "*bis*" condition. It recalls

that a decision on the case must not only have become final but must also have been taken after a determination as to the merits of the case. In view of the subsequent *res iudicata* effect in question, the ECJ clarified that the principle *ne bis in idem* applies once a criminal decision has become final, irrespective of the manner in which that decision became final. As a result, Art. 50 CFR does not preclude subsequent (final) decisions (here: the fine imposed by the German prosecutor) that were adopted after a prior decision (here: the fine imposed by the Italian market authority).

Secondly, the judges in Luxembourg emphasise that the referring court must be sure whether the "*idem*" condition is fulfilled. As consistently stated in previous case law, the two sets of proceedings or the two penalties at issue must relate to an identity of the material facts; mere similarity of facts is not sufficient. The ECJ clarifies several aspects in the present case that the referring court should take into account when it assesses the "*idem*" criterion.

➤ *ECJ on the limitations of the principle ne bis in idem*

The ECJ reiterates its previous case law that, in accordance with Art. 52(1) CFR, limitations on the principle *ne bis in idem* are justified in so far as the limitation is provided for by law and respects the essence of Art. 50 CFR as well as the principle of proportionality. Accordingly, the following issues do not contradict with the essence of the fundamental right and the proportionality:

- Possibility of a duplication of proceedings and penalties under different legislation;
- Authorities can legitimately choose complementary legal responses to certain conduct that is harmful to society, thus they can also pursue distinct objectives of general interest in parallel.

However, it must be ensured that the necessity *stricto sensu* is observed. For this, the following requirements must be fulfilled:

- It must be ensured that the duplication does not represent a burden for the person concerned;
- There are clear and precise rules making it possible to predict which acts or omissions are liable to be subject to a duplication;
- The sets of proceedings in question have been conducted in a manner that is sufficiently coordinated and within a proximate timeframe.

The ECJ affirms for the case at issue that VWAG could have predicted that its conduct was liable to give rise to proceedings and penalties in at least two Member States which followed distinct objectives (unfair commercial practices and administrative offence due to lack of supervision), but – and this is critical – no coordination took place between the German and Italian authorities. This was the case even though the sets of proceedings in question appear to have been conducted in parallel for some months and the German prosecutor had knowledge of the decision at issue at the time when he adopted its own decision. According to the ECJ, difficulties in carrying out a true coordination between authorities being placed in different Member States and working in different branches (administration v law enforcement) does not justify for qualifying or disregarding the coordination requirement. As a result, a legitimate duplication of proceedings and penalties is not possible in the present case.

➤ *Put in focus*

The ECJ comes to the same result as AG *Sanchez Bordona* in its opinion for the case (→eucrim 1/2023, 35–36). Even though the AG recommended that removal of the coordination criterion should be considered, the ECJ maintained it and thus continues its case law on the duplication of administrative and criminal proceedings as established by the three judgments of 2018 in *Menci, Garlsson* and *Di Puma and Zecca* (→eucrim 1/2018, 24–27). It could also have been argued that even a legal basis for the duplication for the two proceedings in questions was not provided and that the essence of Art. 50 CFR has not been ensured (cf. the legal analysis of the case by L. Neumann, eucrim 1/2023, 99–105).

As a result, although the Volkswagen Group has paid the significantly higher fine in Germany, it will likely be spared further sanctions based on the same allegations in the future following the ECJ ruling. The judges in Luxembourg only left one backdoor: it may be doubted that the "idem" requirement (the same facts) was met. This does not seem to be as crystal clear as it appears at first glance. Even the referring court referred to a "similarity" and "homogeneity" of the facts in question. The ECJ indicated that the referring court must verify this issue more clearly by taking into account in its final decision, for instance, that the relaxation of supervision of the activities in Germany is distinct from the marketing and dissemination of misleading advertisement in Italy. It must also be ascertained whether the German prosecutor actually also ruled on the factual elements that gave rise to infringements in Italy; the mere reference to factual elements relating to the territory of another Member States would be insufficient. In this sense, the decision is not yet a complete *carte blanche* for Volkswagen. (TW)

### ECJ Ruled on the Prohibition of Double Jeopardy in Fraudulent Pyramid Schemes

In a case concerning the European arrest warrant (EAW), the ECJ ruled on the scope of the principle *ne bis in idem* in cases of fraudulent pyramid schemes.

In the underlying case (*C-164/22, Juan*), a CEO of two companies is defending himself against his extradition from Spain to Portugal. The CEO used

a company in Spain and a company in Portugal, both of which he controlled, to establish the sale of investment products. The massive uptake of those investment products by individuals allowed the Portuguese company to experience exceptional growth and expansion. Following the intervention of the Spanish judicial authorities in spring 2006, and afterwards that of the Portuguese judicial authorities, the companies ceased their activities, which led to significant financial losses for the investors.

The CEO is serving a prison sentence of 11 years and 10 months in Spain for serious fraud and money laundering. He objects the execution of an EAW issued by Portugal for the purpose of executing a Portuguese sentence of over six years for serious fraud. He claimed that the Portuguese judgment is based on the same facts on which the Spanish judgment is based and therefore the prohibition of double jeopardy applies. The referring High Court of Spain asks the ECJ whether the case involves a single continuing offence, so the CEO is protected by the principle that no one may be tried or punished twice in criminal proceedings for the same criminal offence within the EU.

In its judgment of 21 September 2023, the ECJ ruled that the principle *ne bis in idem* does not preclude the execution of the EAW. The principle *ne bis in idem* is only applicable if the facts for which the person concerned is serving a sentence in a Member State are identical to the facts on which the EAW is based. Thus, there must be a set of concrete circumstances stemming from events which are inextricably linked together in time and space.

According to the ECJ, the use of an identical modus operandi may argue in favour of the "same facts". However, the following circumstances refute this assumption: the activities were carried out via separate legal entities;

**Freezing of Assets**

## The RECOVER Project

The project "RECOVER – Crime Doesn't Pay" (co-funded by the EU Justice Programme 2021–2027) is designed to improve the implementation of Regulation 1805/2018 on the mutual recognition of freezing and confiscation orders – a fundamental cooperation tool in the fight against organised and economic crime. The Regulation has had a strong political value considering its impact in terms of criminal policy and its effect of dragging mutual recognition on substantive issues.

RECOVER is the first impact assessment of the Regulation from a substantive criminal law perspective. Under the coordination of *Anna Maria Maugeri* (full professor of criminal law at the University of Catania/Italy), the project has forged a network of prosecutors, judicial authorities, asset recovery offices, and universities in ten EU Member States. The aim is not only to detect and overcome legal issues in the interpretation of the Regulation but also to establish substantive conditions when implementing it in compliance with the rule of law, all the while increasing mutual trust and harmonisation.

RECOVER consists of the following steps:

- Establishing the subject matter of the Regulation by clarifying the concept of "proceedings in criminal matters" (Art. 1 of the Regulation);
- Identifying the types of freezing and confiscation orders covered by the Regulation in each Member State, including the necessary safeguards;
- Identifying the safeguards in the mutual recognition procedure;
- Pointing out the main obstacles and legal issues regarding implementation of the Regulation and exchanging best practices;
- Assessing the possibility of applying the Regulation to legal persons;
- Identifying the legal and practical difficulties in asset recovery offices' activities;
- Promoting the efficient management of frozen assets, the protection of victims' rights, and social reuse of confiscated assets.

These objectives will be realised by the following means: desk analysis and national reports based on questionnaires by the network partners; workshops as a tool fostering direct dialogue between the partners; and the involvement of non-partner Member States by expert interviews, dissemination workshops, and international seminars with a view towards mutual learning as basis for mutual trust. Best practices, guidelines, and reform proposals will be collected in a comprehensive database to be made available to all EU Member States for successful application of the Regulation. The project partners have carried out the following main activities to date:

- 15 December 2022: Online kickoff meeting for the RECOVER project entitled *"Mutual recognition of freezing and confiscation orders between efficiency and the rule of law"* bringing together the various members of the consortium.
- 31 January 2023: First (online) project workshop entitled "*The concept of proceedings in criminal matters (art. 1 EU Regulation no. 1805/2018) and related safeguards*". The workshop focused on explaining the subject matter of Regulation 1805/2018, in particular interpretation of the concept of "proceedings in criminal matters".
- 13/14 April 2023: Second project workshop in Catania bringing together members of the consortium, members of the advisory and monitoring boards, and other legal experts. The workshop focused on analysing the confiscation models of the European countries involved in the project and on discussing prospects for the harmonisation of their legal systems.

For more detailed information about RECOVER, visit the project website: http://recover.lex.unict.it/.

*Prof. Anna Maria Maugeri*

the fraudulent activity continued in Portugal although investigations were opened in Spain and activity there ceased; the Spanish judgment relates to the investors residing in Spain whereas the Portuguese judgment deals with the detriment of persons residing in Portugal.

On the basis of this interpretative guidance from the ECJ, the Spanish High Court must now decide whether it considers the offenses to be identical. (TW)

### Victim Protection

#### Commission Proposes Reform of Victims' Rights Directive

spot light

On 12 July 2023, the Commission tabled a legislative initiative for amending Directive 2012/29 establishing minimum standards on the rights, support and protection of victims of crime (the Victims' Rights Directive – VRD). The proposal (COM(2023) 424 final) builds on the evaluation of the VRD that was carried out in 2022 and demonstrated the need for targeted amendments to the existing legal framework (→eucrim 2/2022, 119). In addition, in its EU Strategy on Victims' Rights (2020–2025), the Commission committed itself to strengthening the rights of victims of crime in the EU and to reviewing the 2012 VRD (→eucrim 2/2020, 104).

The amendments pursue the following objectives:

- Improving victims' access to information and crime reporting;
- Facilitating access to specialist support for vulnerable victims;
- Ensuring more effective victims' participation in criminal proceeding;
- Improving access to compensation for victims;
- Better aligning victims' protection measures with victims' needs.

The proposed amendments will establish more far-reaching minimum standards to ensure that victims can fully benefit from their rights. The key elements of the proposal are as follows:

- Setting up a universal, EU-wide Victims' telephone helpline (116 006) as well as a comprehensive website with information in most spoken languages, apt for persons with disabilities and with state-of-the art technology also allowing chats and emails;
- Facilitating the reporting of crime, including for victims in detention and irregular migrants;
- Facilitating access to free psychological support especially for all vulnerable victims as long as necessary (i.e., not only in the short term) and depending on the individual needs;
- Strengthening victims' access to support services by requiring support services to remain operational in a crisis;
- Establishing a victim right to assistance in court and enabling victims to challenge decision that affect their rights, independently of their formal status under national law in the criminal proceedings;
- Strengthening the option for victims to participate in criminal proceedings via teleconferencing (i.e., not only in relation to evidence gathering as it is the status quo);
- Reinforcing the rights to compensation by giving victims the right to receive a decision on compensation from the offender only in the course of the criminal proceeding (thus removing the option to have recourse to another proceeding as in the current VRD), and by making it mandatory for Member States to guarantee victims compensation directly and quickly after the judgment;
- Improving victims' individual needs assessment, *inter alia*, by requiring initiation of the individual assessment from the first contact with the authorities and by adding physical protection measures to the list of specialised protection measures;
- Obliging Member States to provide for a possibility for victims to exercise their rights to information and access justice using electronic communication.

The proposal also includes several measures that are designed to ensure adequate and additional support for vulnerable victims, such as children, elderly persons, persons with disabilities, and victims of hate crime. Lastly, the Commission modified the article on the collection, production and dissemination of statistics on victims of crime, in order to improve the completeness, consistency and comparability of data when the VRD is applied.

The proposal is now subject to agreement by the European Parliament and the Council as co-legislators. If adopted, the Commission proposes that Member States would have two years to transpose the amendments into national law; exception: for the use of electronic means of communication, Member States would have four years. (TW)

## Cooperation

### Customs Cooperation

#### Commission Proposes Comprehensive Reform of Customs Union

spot light

On 17 May 2023, the European Commission presented proposals for an ambitious and comprehensive reform of the EU Customs Union. The aim is to simplify customs processes and make them smarter and safer, including by means of an increased use of Artificial Intelligence, a new EU database and a new EU Customs Authority.

According to the proposal, companies wishing to import goods into the EU will be able to submit all information about their products and supply chains once and feed it into a single

online environment: the new EU Customs Data Hub. This will give authorities in all Member States a complete overview of supply chains and the movement of goods in real time. In certain cases, where business processes and supply chains are fully transparent, the most trusted traders ("Trust & Check" traders) will be able to place their goods on the EU market without active intervention by customs authorities and clear all their imports with the customs authorities of the Member State in which they are established. Artificial intelligence will also be used to analyse and monitor data and identify problems.

In order to coordinate Member State controls and investigations, information and expertise will be pooled and assessed at EU level within the new EU Customs Authority. It will act on the data provided through the EU Customs Data Hub. The new regime aims to substantially improve cooperation between customs, market surveillance and law enforcement authorities at EU and national level.

At the same time, the reform will modernise EU customs obligations for e-commerce. Responsibilities will shift from individual consumers and carriers to online platforms. In future, online platforms will have to ensure that customs duties and VAT are paid at purchase, so consumers in the EU can be reassured that all financial duties and EU safety standards for the products are fulfilled.

Furthermore, the reform will abolish the current threshold that allows exemption from customs duties for goods with a value of less than €150. This threshold has been heavily exploited by fraudsters who undervalue the goods to avoid customs duties on import. It is also planned to simplif customs duty calculation for the most common low-value goods bought from outside the EU, reducing the thousands of possible customs duty categories down to only four. This will also reduce the potential for fraud. It is expected that the new tailor-made e-commerce regime will generate additional customs revenue of €1 billion annually.

The Commission proposal is the most comprehensive reform of the EU Customs Union since its establishment in 1968. It delivers on Commission President *Ursula von der Leyen's* promise "to bring EU Customs to the next level". It particularly builds on input by the Wise Person's Group on the Future of Customs.

The legislative proposals will now be debated in the Council of the European Union and the European Parliament for agreement. The European Economic and Social Committee is consulted. (TW)

## Police Cooperation

### New Information Exchange Directive under Criticism

Following the entry into force of Directive 2023/977 on the exchange of information between the law enforcement authorities of Member States (→eucrim 1/2023, 36–39), civil liberties organisation Statewatch voiced criticism over the new legislation. The NGO pointed out that "Europol's data warehouse will grow significantly", because Europol is to receive a copy of all information exchanged when it concerns crimes in its area of responsibility (although Member States should carry out a case-by-case examination as to whether to share data with the agency). In addition, it is regretted that the Union legislator did not take up the request by the EDPS that the single contact points should delete personal data stored in the case management systems soon after the information exchange has taken place. Now, only a decision is to be taken on whether to delete the data or not after a delay of six months. (TW)

## Judicial Cooperation

### German Bar Association Welcomes Proposal for Transfer of Criminal Proceedings But Sees Improvements

There are first reactions to the Commission's proposal of April 2023 for a regulation on the transfer of proceedings in criminal matters (→eucrim 1/2023, 40). In a statement of 12 June 2023, the German Bar Association welcomes the draft regulation in principle. However, it still calls for numerous improvements. For example, the defence's welcoming right to request a transfer risks running out of steam if the authorities are under no obligation whatsoever to decide on such a request and to consider the arguments contained therein. In principle, it is also to be welcomed that, according to the draft, the interests of accused persons are to be taken into account – but there is a lack of a precise formulation of how this interest must be taken into account. Furthermore, there is a lack of enforcement mechanisms and an obligation on the part of the authority to document the extent to which the interests of the accused or suspects have been taken into account in its decision. In the view of the German Bar Association, it is also worthy of criticism that legal remedies are only provided against the acceptance of the transfer, but not against its rejection. (TW)

### ECJ Ruled on Fundamental Rights Refusal of Norwegian Surrender Warrant

spot light

In its judgment of 14 September 2023, the ECJ ruled on the extent Member State courts must take account of fundamental rights when it comes to extradition on the basis of the Agreement on the surrender procedure between, on the one hand, the Member States of the European Union and, on the other hand, the Republic of Iceland and the Kingdom of Norway. In addition, the Court had to

decide as to which extent decisions taken in other EU Member States in the extradition case can be taken into account by the executing court (Case C-71/22, *KT v Sofiyska gradska prokuratura*).

➤ *Facts of the case and questions referred*

The case at issue concerns a surrender procedure before the *Sofiyski gradski sad* (Sofia City Court, Bulgaria). The competent Norwegian authority issued an arrest warrant against KT for fraud which caused damage to the Norwegian social insurance system. When KT entered Poland, KT was arrested on the basis of the respective SIS alert. However, the Warsaw Regional Court (Poland) refused to execute the Norwegian arrest warrant because surrender would entail a breach of Art. 8 ECHR as a result of KT's permanent severance from his children. The Warsaw court also considered that the Norwegian authorities could use other forms of judicial cooperation in criminal proceedings with Bulgaria where KT resides with his children.

Norway upheld the SIS alert and when KT entered Bulgaria he was arrested again. The Norwegian authority issued a new arrest warrant which was based on the same grounds as the first one that was sent to Poland.

In this context, the referring Sofia City Court asked first whether the Agreement on the surrender procedure between the EU and Norway/Iceland allows the issuing of a new arrest warrant in the same case. Second, the referring court raised the question of the possible impact of the refusal previously made by the Polish court.

➤ *ECJ's ruling on successive arrest warrants*

At first, the ECJ stressed that the provisions of the EU-Norway/Iceland Agreement on the surrender procedure are very similar to the corresponding provisions of the Framework Decision 2002/584 on the European Arrest Warrant (FD EAW). No provision in the Agreement prohibits the issuing of several successive arrest warrants against a person, including where the execution of a first arrest warrant has been refused. This is corroborated by the objective of the Agreement that – as the FD EAW – seeks to establish a simplified and more effective system for surrendering persons convicted or suspected of having committed a crime as well as to fight against the impunity of the requested person. A systematic prohibition for the issuing authority to issue a new arrest warrant in the same case would undermine the effectiveness of the established surrender system and would entail a risk of impunity. The ECJ, however, makes two restrictions that must be respected by the *issuing* authority:

- It cannot issue a new arrest warrant if the circumstances have not been changed on the basis of which an executing judicial authority has refused to give effect to the arrest warrant on fundamental rights grounds (Art. 1(3) of the Agreement);
- It must examine whether the issuance of a new arrest warrant is proportional in the light of the particular circumstances. Regarding this proportionality test, the issuing authority must take into account the nature and gravity of the offence for which the requested person is prosecuted, the consequences for that person of the arrest warrant, and the prospects of execution of any new arrest warrant.

➤ *ECJ's ruling on previous refusal by another Member State court*

Since the surrender Agreement and the FD EAW share the same objectives and structure, the ECJ refers to its case law on the FD EAW and calls to mind that, in analogy, the State parties to the Agreement are, in principle, required to execute an arrest warrant issued by another State party and can refuse to execute such arrest warrants only for reasons arising from the Agreement. Refusals on the basis of fundamental rights (Art. 1(3) of the Agreement) can only happen exceptionally and following an appropriate examination of possible infringements. However, the Agreement does not include any provision that provides for the possibility of refusing the execution of an arrest warrant when the execution of a first arrest warrant concerning the same person and the same acts was refused by a State party to that agreement. A refusal on the basis of *ne bis in idem* (Art. 4 No. 2 of the Agreement) does not apply in the constellation referred.

The ECJ clarifies that the refusal decision that exists in an EU Member State (here: the decision by the Warsaw Regional Court) admittedly "*encourages vigilance*" from the executing authority of another Member State (here: the Sofia City Court) to which a new arrest warrant against the same person for the same acts has been addressed. This circumstance is, however, not liable to exempt the executing authority of the latter Member State from its obligation to examine the request for surrender and to take a decision (of its own) on the execution of the arrest warrant.

➤ *Put in focus*

The ECJ's ruling in the case "KT" is interesting in three respects:

First, the judges in Luxembourg interpret the Agreement on the surrender procedure between the EU and Norway/Iceland and the FD EAW largely in parallel. The ECJ case law on the European Arrest Warrant is applied in analogy. This is justified by the reasoning that the two instruments share the same objectives and structure. In this context, the ECJ made clear that the execution of an arrest warrant issued by Norway or Iceland must, in principle, be executed and can only be refused on the basis of the grounds established in the agreement.

Second, the ECJ clarified that the fundamental rights clause in Art. 1(3) in the Agreement (which corresponds to Art. 1(3) FD EAW) established a re-

fusal ground. In parallel to the FD EAW, a refusal on grounds of fundamental rights infringements in the issuing country must, however, be applied narrowly. The ECJ mainly refers here to its recent judgment in *Puig Gordi* →eucrim 1/2023, 41–43.

Third, the ECJ clarified that there is no "mutual recognition of decisions refusing the execution of an arrest warrant". The executing authority that has to deal with a successive arrest warrant issued in the same case against the same person must take a decision on its own. There is no automatic refusal because of a first refusal decision. On the one hand, this decision taken in another Member State (here: Poland) can be considered by the executing authority in the second Member State (here: Bulgaria). On the other hand, the executing decisions must not loose sight of the main objective of the surrender instruments, i.e. avoiding impunity. (TW)

### German Court Denies Extradition to UK Because of Bad Detentions

On 10 March 2023, the Higher Regional Court of Karlsruhe (Germany) declared extradition of a person from Germany to the UK as "currently inadmissible" due to the lack of guarantees for the person's protection of fundamental rights. The decision in an unofficial English translation can be found here.

The requested person's defence council *Dr. Jan-Carl Janssen* put forward objections against extradition with regard to the prison conditions in the UK and a possible violation of Art. 3 ECHR. By also referring to a 2021 CPT report, the Higher Regional Court of Karlsruhe posed several specific questions to the UK authorities with regard to prison conditions to be expected of the prosecuted person after his extradition in the UK. The court requested from the UK binding guarantees that human rights will be respected under international law pursuant to Art. 604 lit. a) and c) of the UK-EU Trade and Cooperation Agreeement (→eucrim 1/2020, 265–271). UK authorities, however, replied rather unspecifically to the questions posed and could not fully discard the substantiated objections raised by the requested person.

The Higher Regional Court of Karlsruhe decided that "it cannot currently be assumed with sufficient certainty that the prosecuted person would receive humane conditions of detention there in the case of his extradition to the United Kingdom and Northern Ireland." The TCA-extradition warrant was revoked. The immediate release of the requested person who was in the prison of Freiburg i.Br., Germany, was ordered. (TW)

### MLA Form for Judicial Cooperation between EU and UK Available

A standard form is now available by which to issue requests for judicial cooperation between the competent authorities of the EU and the UK and Northern Ireland. It was designed by the Specialised Committee established by Art. 8(1)(r) of the Trade and Cooperation Agreement between the European Union and the United Kingdom of Great Britain and Northern Ireland.

The form is available in all EU languages from the Judicial Library on the EJN website. Information about the UK's competent authorities and other important practicalities can also be found in the UK section of the EJN website. (CR)

## European Arrest Warrant

### ECJ: EAW Requires Equal Treatment of Third-Country Nationals

On 6 June 2023, the ECJ delivered an important judgment on the protection of third-country nationals within the regime of the European Arrest Warrant. At the centre was the interpretation of Art. 4(6) of the Framework Decision on the European Arrest Warrant (FD EAW). According to this provision, Member States can confer their judicial authorities the option of refusing to execute an EAW issued for the purposes of executing a custodial sentence or detention order if the requested person is staying in, or is a national or a resident of the executing Member State. The judges in Luxembourg held that the Italian legislation that transposed this provision, but only wishes to apply it to Italian nationals and nationals of other EU Member States (and not to third-country nationals) is incompatible with Union law.

➤ *Facts and background of the case*

The case (C-700/21, *O.G.*) was referred by the Italian Constitutional Court which has to decide on the constitutionality of the Italian national law transposing Art. 4(6) FD EAW. In the concrete case, Italian courts were prevented from refusing the execution of an EAW against a Moldovan (i.e., third-country) national who was sentenced in Romania, even though the person is an Italian resident with stable family and professional life in Italy. The Italian Constitutional Court has doubts as to whether the absolute and automatic exclusion of third-country nationals from benefiting from the FD EAW's optional refusal ground is consistent with Union law. In addition, the court asked about the criteria and conditions demonstrating a sufficient integration in the executing State.

➤ *ECJ on the discriminatory nature of the Italian legislation*

The ECJ, sitting in for the Grand Chamber, first concedes that Art. 4(6) FD EAW confers Member States a margin of discretion. However, if Member States choose to transpose this ground for refusal, this discretion has limits. The transposition must, *inter alia*, comply with the principle of equality in Art. 20 of the Charter of Fundamental Rights of the EU, which requires that similar situations must not be treated differently and that different situations must not be treated in the same man-

ner, unless such different treatment is objectively justified. The requirement that situations must be comparable, for the purpose of determining whether there is a breach of the principle of equality before the law, must be assessed in the light, in particular, of the subject matter and purpose of the act that makes the distinction in question, taking into account the principles and objectives of the field to which the act relates.

The ECJ sees no reason why (socially integrated) third-country nationals would not be in a comparable situation than Italian and EU Member State nationals. This follows mainly from the wording of Art. 4(6) FD EAW, which makes no distinction with regard to nationality, and the objective, i.e., increasing the requested person's chances of reintegrating into society.

Therefore, the Italian law excluding third-country nationals from the scope of the refusal ground, even where those third-country nationals are staying or resident in the territory of the executing Member State and without account being taken of their degree of integration within the society of that Member State, is not in line with Art. 20 of the Charter.

The judges in Luxembourg clarified, however, that Member States can lay down the condition that the person concerned has stayed continuously in that State for a minimum period of time. Furthermore, they stressed that Art. 4(6) FD EAW has three requirements:

- Determination whether a person, who is not an own national of the executing country, "is staying or resident" in that State;
- There is a legitimate interest to justify that the custodial sentence or detention order of the issuing State is enforced on the territory of the executing Member State;
- The executing Member State enforces the foreign sentence/detention order in accordance with its domestic law.

➤ *ECJ on assessment of sufficient connection to the executing Member State*

The ECJ stated that, in order to assess whether it is appropriate to refuse to execute the EAW issued against a third-country national who is staying or resident in the territory of the executing Member State, the executing judicial authority must make an overall assessment of all of the specific elements characterising the situation of the requested person. These elements must be capable of showing that there are connections between that person and the executing Member State that may lead to the conclusion that the person concerned is sufficiently integrated into that State. Those elements include the family, linguistic, cultural, social or economic links that the third-country national has with the executing Member State as well as the nature, duration and conditions of his or her stay in that Member State.

➤ *Put in focus*

By its judgment of 6 June 2023, the ECJ first clarified that legislation of EU Member States transposing the Framework Decision on the European Arrest Warrant must respect the Union's fundamental rights enshrined in the Charter (here: principle of equality before the law). Persons staying or being a resident of the executing Member State are protected from being extradited under the condition that the sentence at issue is executed by the that Member State. Discretion for the judicial authorities in the executing Member State is limited to the examination of a "legitimate interest" of enforcing the sentence or detention order of the issuing State. The ECJ also clarified that the elements of this assessment also apply to the assessment determining whether the requested person "is staying" in the executing Member State.

Second, the ECJ made clear that the European Arrest Warrant does not only pursue the aim of law enforcement, but also the aim of social rehabilitation of an individual. In this context, the EAW coincides with Framework Decision 2008/909/JHA on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union. (TW)

### ECJ Ruled on Consequences of the Prosecutor's Lacking Independence for the Consent Procedure

On 6 July 2023, the ECJ clarified the consequences to be drawn from its case law on the lacking independence of public prosecution services so that they cannot be recognised as "issuing judicial authority" within the meaning of Art. 6(1) of the Framework Decision on the European Arrest Warrant (FD EAW). The questions raised concerned the interpretation of the consent as an exception of the speciality principle in EAW cases (Case C-142/22, *OE v Minister for Justice and Equality*).

In the case at issue, OE opposed decisions by Irish courts to grant consent to a request by the Netherlands to prosecute OE for offences committed prior to his surrender other than those which provided the justification for the initial Dutch European arrest warrants. He argued that the initial EAWs were issued by Dutch public prosecutors who due to their subordination to the executive cannot be regarded as "issuing judicial authority" in accordance with the requirements arising from FD EAW and the respective CJEU case law (→eucrim 1/2019, 31–33 and eucrim 4/2020, 292–293). According to OE, this fact also precludes the request for consent in the framework of Art. 27(3) lit. g) and (4) FD EAW.

The referring Supreme Court of Ireland is uncertain whether OE can raise this argument and argued that the legal classification of the relationship between the surrender procedure and the consent procedure decides on

whether the Irish courts must apply the principle of estoppel.

The ECJ decided that the consent decision has a subject matter that is specific to it. Therefore, the examination by the executing authority is separate from and independent of the examination prompted by the European arrest warrant.

The ECJ concludes that Art. 27(3) lit. g) and (4) FD EAW must be interpreted as meaning that the fact that an EAW on the basis of which a person has been the subject of a surrender decision has been issued by an authority, which did not constitute an "issuing judicial authority" within the meaning of Art. 6(1) FD EAW, does not preclude the executing judicial authority from subsequently giving its consent to that person being prosecuted, sentenced or otherwise deprived of his or her liberty for an offence committed prior to his/her surrender other than that for which he/she was surrendered. (TW)

### AG: Best Interest of Child Must Guide Decision to Execute EAW

**spot light**

On 13 July 2023, Advocate General Tamara Ćapeta presented her views as to which extent the best interest of the child is relevant for the execution of a European Arrest Warrant (EAW).

➤ *Facts of the case and question referred*

In the underlying case (C-261/22, *GN*), the Supreme Court of Cassation in Italy has to deal with the question of whether a mother of a young child can be extradited to Belgium where she has to serve a sentence of five years' imprisonment. Italian judicial authorities found that – due to a lack of replies from the part of Belgian authorities – there is no certainty that Belgian law recognised custody arrangements comparable to those in Italy, which protect a mother's right not to be deprived of her relationship with her children and to ensure that children receive the necessary maternal and family assistance. These rights are guaranteed by the Italian Constitution, Art. 3 of the Convention on the Rights of the Child, and Art. 24 of the Charter of Fundamental Rights of the EU.

The Supreme Court of Cassation seeks guidance from the ECJ whether it is entitled to refuse or postpone the execution of an EAW if by such a surrender it risks breaching the fundamental rights of a mother whose surrender is requested as well as the fundamental rights of the minor children living with her.

➤ *AG's Opinion and reasoning*

According to AG *Ćapeta,* refusal of an EAW on grounds of fundamental rights is only possible if there are systemic or generalised deficiencies in the issuing state (here: Belgium) with regard to ensuring the right to family life of prisoners. Since there are no indications of such systemic and generalised deficiencies, the Italian authorities cannot refuse the execution of the EAW on the ground of a possible breach of the woman's/mother's fundamental rights.

Referring to the ECJ case law in the area of asylum, AG *Ćapeta* found, however, that the decision on the EAW must take account of the fundamental right of the children, i.e., the best interest of the child which is protected in the Charter. There is nothing in the FD EAW that precludes the recognition of this interest and implement it as a refusal ground.

However, before refusing the EAW, the executing authority (here: the Italian courts) must determine the concrete situation of the child and communicate with the issuing authority (on the basis of the mechanism established in Art. 15(2) FD EAW). Refusal is only possible if the executing authority has sufficient information that would allow it to be absolutely certain that the execution of the EAW would go against the best interest of the child.

The AG adds that the ECJ must reconcile the aim of ensuring the best interests of the child with the aim of avoiding impunity, one of the main aims of the EAW system. In doing so, she proposes applying Art. 4(6) FD EAW that regulates situations in which persons staying in the executing Member State need not be surrendered if the executing State undertakes the execution of the prison sentence on its territory. Even though this article provides discretion for the executing Member State, it might turn into an obligation if the best interests of the child must be safeguarded, the AG notes. She advocates that Art. 4(6) FD EAW would be the best option for the mother not to leave the country while the relationship with her child can be maintained.

The AG also concludes that temporarily postponing surrender under Art. 23(4) FD EAW is no option in the case at hand. (TW)

## Law Enforcement Cooperation

### Results of EncroChat Take-Down

Two years after the dismantling of the encrypted communications tool EncroChat, which had been widely used by organised crime groups (→eucrim 1/2021, 22–23), law enforcement and judicial authorities are still reaping the rewards. On 27 June 2023, French and Dutch judicial and law enforcement authorities presented a first overview of the results. Based on the information retrieved from the dismantled tool, investigators managed to intercept, share, and analyse over 115 million criminal conversations involving an estimated number of over 60,000 users worldwide.

After more than 6500 arrests worldwide and close to €900 million seized in criminal funds, the take-down of EncroChat can be considered a major success in countering organised crime. In total, courts convicted criminal to 7,134 years of imprisonment up to now. The press release on the first

results of the EncroChat operation also provides background information about the dismantling process and the law enforcement cooperation also involving Eurojust and Europol. (CR)

### Legislation on JIT's Collaboration Platform Passed

After approval by the European Parliament and the Council, Regulation (EU) 2023/969 on establishing a collaboration platform to support the functioning of joint investigation teams and amending Regulation (EU) 2018/1726 was published in the Official Journal L 132/1 of 17 May 2023. The legislative proposal was tabled by the European Commission in January 2022 (→eucrim 4/2021, 204).

The responsibility for designing, developing, and operating the platform will be entrusted to eu-LISA, the EU agency responsible for the operational management of large-scale IT systems in the area of freedom, security, and justice. The platform aims to facilitate and improve the day-to-day coordination and management of joint investigation teams (JITs). JITs are set up by two or more States for specific criminal investigations with a cross-border impact and for a limited period of time. The platform will be connected to the authorities participating in the JITs in order to ensure electronic exchange of information and evidence and electronic communication. Use of the platform is not mandatory, but strongly encouraged by the Union legislator.

The platform should also support the European authorities Europol, Eurojust, OLAF, EPPO and other competent Union bodies, offices and agencies or representatives of an international judicial authority that participate in a JIT. They will have access to the platform to the extent necessary for the performance of the tasks set out in the relevant legal acts establishing them, albeit limited to duly authorized staff members.

A cautious approach was finally chosen for the inclusion of customs officials. They can have access to the JIT collaboration spaces, if they are members of JITs set up pursuant to Framework Decision 2002/465/JHA. Germany had lobbied strongly for extending the scope to customs, especially in the Council.

The Regulation entered into force on 6 June 2023. The operational start of the platform will be determined by the Commission. A respective decision should be taken no later than 7 December 2025. (SH)

### Fourth JITs Evaluation Report

At the beginning of June 2023, the Secretariat of the Network of National Experts on Joint Investigation Teams (JITs) published its Fourth JITs Evaluation Report since 2014, offering an overview of practical findings, lessons learned, and best practices in conjunction with the use of JITs over the past several years. The report is based on 82 evaluations completed by JITs practitioners between November 2019 and November 2022.

According to the report, a number of best practices regarding the setting-up phase of JITs could be identified:

- Early meetings between law enforcement and judicial authorities from the countries concerned;
- Flexibility regarding the location of coordination meetings;
- The early involvement of other authorities, Eurojust, and other relevant EU agencies and bodies;
- The involvement of liaison prosecutors where relevant;
- Flexibility regarding the language(s) of the JIT agreement;
- The early explanation of the national legal/judicial systems in order to pre-empt potential hindrances to cooperation.

For the operational phase, best practices identified include, for instance:

- Direct and continuous contact and exchange of information among JIT parties;
- The establishment of personal relationships between JIT members, and the appointment of contact points;
- The exchange of information on specificities of the different legal systems;
- The appointment of seconded members;
- The use of the same interpreters throughout the JIT;
- Coordination of media strategy;
- Communication about JIT funding;
- Mid-term evaluations of cooperation within the JIT;
- Extension of cooperation into the trial phase to allow for efficiency in additional gathering and sharing of information and evidence (if possible according to national legislation);
- The participation of victims of crime in the assessment process.

Other chapters of the Fourth JITs Evaluation Report describe Eurojust's experience with multilateral JITs. There is also a dedicated checklist in all EU official languages, which gives an overview of what needs to be taken into account in the setting-up and operational phases of a multilateral JIT. Lastly, the report presents general figures as well as important innovations, trends, and new practices in the functioning of JITs. It also provides insight into judicial decisions into how some Member States tackled JITs-related issues. (CR)

The operation was part of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) – a recurring four-year cycle to identify, prioritise, and address threats posed by organised and serious international crime. (CR)

### E-evidence Regulation and Directive Published

After five years of negotiations, the Council and the European Parliament (EP) finally adopted the legislative acts that will **introduce a new system for the gathering of electronic evidence** in criminal proceedings in the EU. For the initial Commission proposal – the so-called e-evidence package →eucrim 1/2018, 35–38. eucrim has continuously reported on the progress of this legislative initiative and the stakeholders' criticism against it. After having reached political agreements in January 2023 (→eucrim 1/2023, 45), the legislation was **published in the EU Official Journal** at the end of July 2023. The new rules on e-evidence consist of two legislative measures:

- Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (*O.J.* L 191, 28.7.2023, pp. 118–180);
- Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (*O.J. L 191, 28.7.2023, pp. 181–190*).

In order to apply the rules in a consistent manner and to provide time for implementation and compliance, the **Regulation applies from 18 August 2026.** The **Directive** must be **transposed** into the national laws of the EU Member States **by 18 February 2026.**

The **main aim** of the new EU legislation is to have in place an alternative – quicker and more efficient – mechanism to the existing international cooperation and mutual legal assistance tools in order to specifically address the problems stemming from the volatile nature of e-evidence and the "loss of location" aspect of stored data.

The Regulation lays down the rules under which an authority of a Member State, in criminal proceedings, may issue a European Production Order or a European Preservation Order and thereby (directly) order a service provider offering services in the Union and established in another Member State, or, if not established, represented by a legal representative in another Member State, to produce or to preserve electronic evidence regardless of the location of the data.

The Directive lays down the rules on the designation of designated establishments and the appointment of legal representatives of certain service providers that offer services in the Union, for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States, for the purposes of gathering electronic evidence in criminal proceedings.

➤ *Summary*

The following summarises the key features of the pieces of legislation by way of "Q&A":

➤ *Who is the addressee of the Regulation?*

The Regulation applies to **service providers which offer services in the Union.** These notions are defined broadly.

For the purposes of the Regulation, a **service provider** is anyone providing one or more of the following categories of services (except for financial services):

- Electronic communication services, such as:
  - internet access services,
  - interpersonal communications services (e.g., messaging services, email services and internet telephony services);
  - Internet domain name and IP numbering services, such as IP address assignment, domain name registries, and related privacy and proxy services;
  - Other information society services which enable users to communicate with each other, or to store or otherwise process data, such as social networks, online marketplaces and other hosting service providers.

**"Offering services in the Union" means:**

- enabling natural or legal persons in a Member State to use the aforementioned services; and
- having a *substantial connection*, based on specific factual criteria, to the Member State referred to in the first point; such a substantial connection is to be considered to exist where the service provider has an establishment in a Member State, or, in the absence of such an establishment, where there is a significant number of users in one or more Member States, or where there is targeting of activities towards one or more Member States.

➤ *What is the scope ratione materiae?*

European Production Orders and European Preservation Orders may be issued only in the framework and for the purposes of **criminal proceedings,** and for the execution of a custodial sentence or a detention order of at least four months, following criminal proceedings. It is a condition that the sanction was not imposed by a decision that was rendered in absentia, in cases where the person convicted absconded from justice.

Such orders may also be issued in proceedings relating to a criminal offence for which a **legal person** could be held liable or punished in the issuing State. Considering that legal notions of EU law are to be interpreted autonomously, "criminal proceedings" in this context could also mean administrative fine proceedings against corporates in which offences are at issue; this mainly concerns countries that do not know a corporate criminal law, such as Germany.

➤ *What are European Production and Preservation Orders?*

The **Production Orders** allow law enforcement authorities in one EU Member State to request electronic data from service providers (established or represented in another EU Member State) and hand them over.

**Preservation Orders** can be issued by law enforcement authorities to oblige service providers to preserve electronic data that can later be requested for production, so that the data are prevented from being deleted or overwritten.

➤ *Which data are covered?*

European Production and Preservation Orders can be issued for **subscriber, traffic, and content data** as traditionally defined (see also Art. 3(9), (11), and (12) of the Regulation). In addition, the Regulation introduces a fourth category of data, i.e., "**data requested for the sole purpose of identifying the user**". This category is defined as "IP addresses and, where necessary, the relevant source ports and time stamp, namely the date and time, or technical equivalents of those identifiers and related information, where requested by law enforcement authorities or by judicial authorities for the sole purpose of identifying the user in a specific criminal investigation".

The Regulation only applies to data that has already been stored, i.e., it does **not** apply to data allowing **live monitoring** and data that will be created in the future.

➤ *Who can issue the Orders?*

- A judge, a court, or an investigating judge competent in the criminal case can issue all kinds of orders for all types of data that can be requested as electronic evidence (see supra);
- Other designated investigating authorities in criminal proceedings can also issue orders, but they must be validated by the judicial authorities referred to in the first point before transmission;
- Public prosecutors can issue European Production Orders to obtain subscriber data and "data requested for the sole purpose of identifying the user" (see above) as well as European Preservation Orders. For such orders, the public prosecutor is also a competent authority to validate orders from other investigating authorities (in addition to a judge, a court, or an investigating judge). If a public prosecutor wishes to obtain traffic and content data, his/her order must be validated by a judge, a court, or an investigating judge.

➤ *Which crimes can the Orders be issued for?*

- A European Production Order to obtain subscriber data or data requested for the sole purpose of identifying the user (see above), may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least four months;
- A European Production Order to obtain traffic or content data may be issued for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least three years, or – regardless of this threshold – a specific set of offences connected with cyber-crime, fraud relating to non-cash means of payment, terrorism and sexual abuse of children.
- A European Preservation Order may be issued for all criminal offences, "if it could have been issued under the same conditions in a similar domestic case", and for the execution of a custodial sentence or a detention order of at least four months.

➤ *Which deadlines apply?*

In **regular cases**, the service provider must transmit the requested electronic evidence to the issuing authority within **10 days** following receipt of the European Production Order Certificate (EPOC). In **emergency cases**, the service provider has **8 hours** for transmitting the requested electronic data.

If **preservation** is requested, the service provider is obliged to preserve the data for **60 days**. The issuing authority can extend this period by an additional 30-day period.

➤ *What responsibilities does the issuing authority have?*

- Looking at the most important instrument, i.e., the European Production Order, the issuing authority must assess the necessity and proportionality to the case at hand. It must take into account the rights of the suspect or the accused person in proceedings relating to a criminal offence and should only issue a European Production Order if such order could have been issued under the same conditions in a similar domestic case.
- The Order must include specific information and justifications, which are listed in Art. 5(5) of the Regulation.
- The issuing authority must verify legal situations, under which the issuance of European Production Orders is limited or excepted. This refers to (1) European Production Orders European Production Orders for all data categories if parallel criminal proceedings are ongoing in another Member State (*ne bis in idem* situations), and (2) European Production Orders for traffic and content data if:
  - data are protected by **professional privilege** under the law of the issuing State (Art. 5(9) of the Regulation);
  - data protected by **immunities or privileges** under the law of the enforcing State, including data subject to rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media under the law of the enforcing State (Art. 5(10) of the Regulation).
- In case of a European Production Order for traffic and content data, the issuing authority must notify the enforcing authority (i.e., the competent authority in the State, in which the service provider is established or its legal representative resides) if the data subject or crime is outside the is-

suing State's jurisdiction (cf. Art. 8 of the Regulation).

■ The issuing authority must review the European Production Order if the service provider raises grounds not to enforce the Order (cf. Art. 10(5)-(9), Art. 17 of the Regulation).

■ The issuing authority must inform the targeted person without undue delay about the production of data (cf. Art. 13 of the Regulation). Delaying and restricting the information for a limited period is possible in accordance with Art. 13(3) of Directive 2016/680).

➤ *What obligations do service providers have?*

■ Service providers offering services in the EU must designate or appoint at least one addressee for the receipt of, compliance with and enforcement of European Production and Preservation Orders (in accordance with Art. 3 of the Directive).

■ Designated establishments or legal representatives of the service provider must be staffed with the necessary powers and resources to comply with the Orders (Art. 3(4) of the Directive).

■ The service providers must produce the data within the set deadlines (see supra). If a European Preservation Order is received, data must be preserved without undue delay and be kept for the set period (see supra).

■ The service provider has information obligations vis-à-vis the issuing and enforcing authority if it intends to raise objections to comply with the Orders (cf. Art. 10, Art. 11 of the Regulation).

■ The service provider is subject to possible sanctions for non-compliance.

■ The service provider must ensure confidentiality, secrecy and integrity of the data produced and preserved (cf. Art. 13(4) of the Regulation).

➤ *What rights do service providers have?*

■ The service provider can seek clarification from the issuing authority if the European Production Order is incomplete, contains manifest errors or insufficient information (cf. Art. 10(6) of the Regulation).

■ The service provider can raise two legal grounds not to comply with a European Production Order:

- Immunities and privileges (see supra and Art. 10(5) of the Regulation);
- Conflict with an obligation under the applicable law of a third country (Art. 17(1), (2) of the Regulation).

➤ *What responsibilities does the enforcing authority have?*

■ The enforcing authority in the enforcing State is entitled to evaluate orders by the issuing state and to decide on their recognition, either when it was simultaneously notified (cf. supra and Art. 8 of the Regulation) or requested by the service providers, or during the enforcement procedure (if the service provider does not comply with a European Production or Preservation Order – Art. 16 of the Regulation).

■ The enforcing authority can raise the following grounds for refusal (Art. 12 of the Regulation) if it was notified (i.e., cases of European Production Orders for traffic and content data and the data subject or crime are located outside the issuing State, cf. supra):

- Immunities and privileges granted under the law of the enforcing State;
- In exceptional situations, manifest breach of fundamental rights set out in Art. 6 TEU and the CFR;
- Ne bis in idem;
- Double criminality requirement not fulfilled unless the European Production Order concerns a listed offence with a specific threshold (Art. 12(1)(d) and Annex IV of the Regulation).

■ Grounds for refusal pursuant to Art. 12 must be raised within specific deadlines (10 days following receipt of the notification in regular cases, and 96 hours following such receipt in emergency cases).

■ Before deciding to raise a ground for refusal, the enforcing authority must contact the issuing authority and negotiate a solution.

■ The enforcing authority must ensure enforcement of legitimate orders in accordance with the detailed rules stipulated in Art. 16 of the Regulation.

➤ *What rights does the targeted person/suspect have?*

■ A suspect or an accused person (or his/her lawyer) can request the issuing of a European Production or Preservation Order "within the framework of applicable defence rights in accordance with national criminal procedural law" (Art. 1(2) of the Regulation).

■ The person whose data are being requested (targeted person) has the right to be informed of the production of data by the issuing authority unless a reason for delaying or restricting the information applies on the part of the issuing authority (Art. 13 of the Regulation).

■ The targeted person must have the right to effective remedies against the order before a court in the issuing State (cf. Art. 18 of the Regulation).

➤ *How are conflicts of law resolved?*

The Regulation provides for a special review procedure (Art. 17) if a service provider considers that compliance with a European Production Order would **conflict with an obligation under the law of a third country**. After the service provider had filed a "reasoned objection" (no later than 10 days after receipt of the EPOC) and duly informed the issuing and enforcing authorities, the issuing authority reviews its order and decides to uphold or withdraw it. If the issuing authority upholds the order, it must request a **review by a competent court of the issuing State**. The execution of the European Production Order is suspended pending completion of the review procedure at court. If the court has found that the law of the third country is applicable and prohibits disclosure of the data concerned, the court would not automatically lift the European Production

Order but has to assess the interests at stake and take a **balancing decision**. The relevant factors are provided in Art. 17(6) of the Regulation.

➤ *Can service providers be sanctioned?*

According to the **Regulation**, Member States must lay down **pecuniary penalties** if service providers infringe the rules on the execution of European Production and Preservation Orders. It must be ensured that pecuniary penalties of up to 2% of the service provider's total worldwide annual turnover can be imposed.

Infringements of the national rules transposing the **Directive** require Member States to lay down "**effective, proportionate and dissuasive penalties**" and take all measures necessary to ensure that they are implemented. In addition, Member States must annually report non-compliant service providers to the Commission.

➤ *Put in focus*

The e-evidence Regulation and Directive is the result of a hard compromise found in trilogue negotiations between the European Parliament, the Council and the Commission---. It reflects the difficult exercise to appropriately balance the interests for smooth law enforcement on the one hand and for adequate protection of fundamental rights and against misuse in favour of the individual on the other. The new legal instruments provide for more paths for law enforcement authorities to move the case forward despite obstacles prevalent in other jurisdictions.

Issues to reject the enforcement of orders from foreign jurisdictions are widely removed and, in essence, only exist in case of traffic and content data. The involvement of the enforcing State, for which the EP fiercely stood up, was limited at the end, since the notification requirement was made subject to several requirements. Given these limits and the tight deadlines, it can be questioned whether the Orders can be effectively reviewed. Practice will demonstrate whether the new rules to gather electronic evidence in the bloc are a progress and lead to the often proclaimed "paradigm shift" regarding cooperation in the EU.

In addition, it remains to be seen whether the EU's new e-evidence rules are apt for a model in other States or in multilateral conventions at the international level.

It is also noteworthy that the e-evidence Regulation and Directive is one component of other recent EU regulations addressing online law enforcement. This includes, for instance, the EU Digital Services Act (DSA), which introduced responsibilities and a system of accountability and transparency for providers of intermediary services (→eucrim 4/2022, 228–230), and Regulation 2021/784, which regulates the duties of care to be applied by hosting service providers to remove or disable access of terrorist content online (→eucrim 2/2021, 95–97).

➤ *Criticism*

Stakeholders fought until the end to stop the e-evidence Regulation. In an open letter of 12 June 2023, civil society, doctors, lawyers and journalists associations and internet service providers called on the EP to reject the "e-evidence package" since it risks to "severely undermine fundamental rights" and fails to provide legal certainty. It is regretted that the EP's improvements in first drafts did not last during negotiations with the Council. In addition, the associations criticised that the Regulation would set a terrible precedent for the level of protection when law enforcement authorities across the world order access to people's personal data from private entities in the EU. They found the following elements particularly concerning:

- Basically toothless notification system;
- Failure to account for national contexts with weakened rule of law and heightened risks of political repression;
- Poorly designed safeguards regarding professional secrecy and confidentiality;
- Limited right to effective remedies by insufficiently regulated "gag orders", weak rules for onward transfers and many barriers for individuals who defend themselves in front of a court.

In a press release of 13 June 2023, the European Broadcasting Union (EBU) commented: "Even though a few safeguards in relation to media freedom were introduced, we fear that the final text could still be misused to get hold of confidential data belonging to journalists."

NB: For a detailed analysis of the "e-evidence package" and its connection with other international developments →articles in this issue, pp. 169–240. (TW)

# Articles

## Articles / Aufsätze

### Fil Rouge

On 12 July 2023, the EU adopted the "e-evidence package", a legislative initiative composed of a Regulation and a Directive designed to significantly facilitate access to electronic evidence by law enforcement in criminal investigations. It is a culmination of five-year long negotiations and even longer debates on an issue resulting from a clash between the limitations of enforcement jurisdiction linked to state territory and the borderless nature of cyberspace. The new instruments constitute nothing less than a legal revolution allowing law enforcement authorities to address binding cross-border requests to produce data directly to private actors: the service providers. The adoption of the package, however, is only a first step, albeit a pivotal one, on the path towards solving the e-evidence conundrum. It foresees a three-year period for the necessary adaptation of national laws to the Regulation and the implementation of the Directive as well as for the creation of the technical infrastructure required to safely exchange data. The effectiveness of this new solution at the EU level will also depend on an agreement, still to be negotiated with the USA, allowing the US providers to transfer data to EU law enforcement without engaging US judges. Another piece of the e-evidence puzzle is the 2nd Protocol to the Cybercrime Convention, which also offers new possibilities to issue cross-border requests for data directly to service providers and has been open for signature since 2022. It has already been signed by almost 50 countries but only ratified by two so far.

It is the second issue of *eucrim* dedicated to electronic evidence, the first one – 4/2018 – examined those problems at the start of the legislative process, when the proposal for the e-evidence package was published. This issue studies the outcome of the legislative process and provides an outlook on future challenges and unaddressed problems still to be tackled.

In the first article, *Kristin Pfeffer* presents an overview of current national, European, and international legal efforts to regulate cross-border access to electronic evidence. The second article by *Gianluca Forlani* zooms in on the EU e-evidence package, giving an overview of the lengthy negotiation process for this controversial legislative proposal. The e-evidence package is assessed in detail in the contribution by *Adam Juszczak and Elisa Sason,* who offer a thorough look at the new instruments and their implications for private actors and international cooperation, in particular with the USA. In the fourth article, *Pavlos G. Topalnakos* takes a critical view of the new Regulation, pointing out problems that may arise in execution of the European Production Order, resulting in potential violations of individuals' rights. The next article by *Maria Ludwiczak Glassey* juxtaposes the European Production Orders with the solutions applicable in Swiss law; she also reflects on the rules for the exchange of electronic evidence between Switzerland and EU Member States. The sixth contribution by *Alexandru Frunza-Nicolescu* presents the current legal (European and international) framework for collection of electronic evidence by the EPPO, examining different configurations of the EPPO's participating and non-participating States.

Two articles analyse areas beyond the area of application of the new legal framework on e-evidence in criminal matters. *Stanisław Tosza* explores the question of gathering electronic evidence for punitive administrative proceedings, which has so far remained under the radar. He presents a recent research initiative on these problems, examined not only in the context of OLAF's competencies and PIF proceedings but also as regards customs, tax, competition, and GDPR enforcement. In the eighth article, *Lorena Bachmaier* makes a case for the need to take legislative action at the EU level on the harmonisation of mutual admissibility of evidence and electronic evidence in criminal proceedings. She presents the recent proposal for a directive in this matter prepared under the auspices of the European Law Institute.

The current issue also offers insights into topics dealing with additional current issues that have triggered debate in two important areas. *Hans-Holger Herrnfeld* reviews the AG's opinion concerning the first preliminary ruling request on the EPPO Regulation regarding interpretation of its Art. 31 on cross-border investigations. The contribution by *Vagelis Papakonstantinou* and *Evangelos Zarkadoulas* focuses on the issue of remote biometric recognition and emotion inference applications in the context of negotiations on the AI Act, in particular critically examining the position of the EU Parliament.

*Prof. Dr. Stanisław Tosza,* Associate Professor in Compliance and Law Enforcement, University of Luxembourg

# Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln

## Aktuelle nationale, europa- und völkerrechtliche Entwicklungen

Kristin Pfeffer

**This article provides an overview of current national, European, and international legal efforts to regulate cross-border access to electronic evidence. At the level of the EU, it was recently decided to harmonise the legal systems of the Member States by means of regulations and directives, which is to be flanked by an agreement between the EU and the USA in the future. In addition, there are already agreements under international law, such as the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention) of the Council of Europe. Meanwhile a future UN Cybercrime Convention is being negotiated in the UN. This article outlines these developments.**

### I. Einleitung

Die Fallzahlen im Bereich der Internetkriminalität steigen im Zuge der weltweiten Digitalisierung auch in Europa stetig an. Laut Europäischem Rat lag der Anteil strafrechtlicher Ermittlungen, die digitale Daten zum Gegenstand hatten, bereits 2018 bei 85 Prozent, gegenwärtig ist der Prozentsatz noch höher.[1] Zur Verfolgung dieses regelmäßig grenzüberschreitenden Phänomens[2] sind die Strafverfolgungsbehörden bei ihren Ermittlungen auf die Zusammenarbeit mit ausländischen Stellen angewiesen. Somit werde, so heißt es weiter in dem Bericht des Europäischen Rates, in über 50 Prozent aller strafrechtlichen Ermittlungen ein Rechtshilfeersuchen gestellt, um elektronische Beweismittel zu erhalten.[3]

Doch obwohl es durchaus erfolgreiche Ermittlungen gegen grenzüberschreitend agierende Täter im Internet gibt, werden die meisten Verfahren eingestellt, weil die dafür erforderlichen justiziellen Rechtshilfeersuchen-Prozesse zu lange andauern und häufig im Sande verlaufen.[4] Deshalb werden sowohl auf nationaler als auch europäischer und völkerrechtlicher Ebene neue rechtliche Lösungen gesucht: So wurden von deutschen Gerichten vereinzelt die vorhandenen nationalen Ermächtigungsgrundlagen weit ausgelegt (dazu unter II.). Auf der Ebene der EU-Mitgliedstaaten wurde jüngst eine Harmonisierung der mitgliedstaatlichen Rechtsordnung im Verordnungs- und Richtlinienwege beschlossen, was künftig mit einem Abkommen zwischen der EU und den USA (dazu unter III.) flankiert werden soll. Daneben gibt es bereits völkerrechtliche Abkommen, wie das zweite Zusatzprotokoll zur Cybercrime-Konvention des Europarates (siehe IV). Inzwischen wird auch in der UN eine künftige UN-Cybercrime-Konvention ausgehandelt (siehe V).

### II. Weite Auslegung vorhandener nationaler Vorschriften (Beispiel Deutschland)

Ein Ansatz, zeitaufwendige Rechtshilfegesuche zu vermeiden, ist die extensive Auslegung der Erlaubnis zur Online-Durchsicht elektronischer Speichermedien im Strafprozessrecht nach § 110 Abs. 3 StPO.[5]

Dem Wortlaut nach erlaubt § 110 Abs. 3 StPO den offenen Zugriff auf räumlich getrennte Speichermedien. Die Regelung dient dazu, den Verlust beweiserheblicher Daten zu vermeiden, die von dem durchsuchten Computer aus zwar zugänglich sind, sich aber auf einem räumlich getrennten Speichermedium, wie etwa dem Server im Intra- oder Internet, befinden.

Nach Auffassung des LG Koblenz etwa stellt der Zugriff auf Daten von Cloud-Nutzern stets eine rein inländische Ermittlungsmaßnahme im Sinne des § 110 Abs. 3 S. 2 StPO dar, unabhängig vom Speicherort. Jedenfalls bei Cloud-basierten Speicherdiensten sei ein Ermitteln des aktuellen Speicherorts regelmäßig nicht zielführend, sodass ein Zugriff inländischer Ermittler:innen auch auf im Ausland gespeicherte Daten erfolgen könne. Infolge des regelmäßig nicht bekannten Speicherorts sei jedenfalls keine willkürliche Missachtung ausländischer Hoheitsrechte anzunehmen und damit kein Beweisverwertungsverbot die Folge.[6]

Die herrschende Ansicht in der Rechtswissenschaft sieht in einer solchen Maßnahme hingegen eine Überschreitung der Grenzen des § 110 Abs. 3 S. 2 StPO und einen Verstoß gegen das Recht des Beschuldigten auf ein faires Verfahren, welches zu einem Beweisverwertungsverbot führe.[7]

## III. E-Evidence-Gesetzgebungspaket der EU und Abkommen mit den USA

Im Juni 2023 hat die EU das Gesetzgebungspaket zur grenzüberschreitenden Sicherung und Herausgabe elektronischer Beweismittel verabschiedet, das seit Vorlage durch die Europäische Kommission im Jahr 2018 heftig diskutiert wurde. Vollständig in Kraft treten werden die Regeln erst in rund drei Jahren. Das Paket besteht aus der Verordnung über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen[8] und der Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren.[9]

Die neuen Vorschriften ermöglichen es nationalen Strafverfolgungsbehörden, Beweismittel direkt von Diensteanbietern in anderen Mitgliedstaaten anzufordern (sog. „Herausgabeanordnungen") oder die Aufbewahrung von Daten für bis zu 60 Tage zu verlangen, damit relevante Daten nicht zerstört werden oder verloren gehen (sog. „Sicherungsanordnung"). Es wird auch eine verbindliche Frist von 10 Tagen für die Beantwortung einer Herausgabeanordnung eingeführt; in Notfällen ist die Frist auf 8 Stunden reduziert.

Diese Anordnungen können sich auf alle bei den Online-Diensten gespeicherten Daten beziehen, z.B. auf Teilnehmer-, Verkehrs- und Inhaltsdaten. Für Verkehrsdaten (außer für Daten, die ausschließlich zur Identifizierung der Nutzer angefordert werden) und für Inhaltsdaten wurde eine Einschränkung vorgesehen. Diese Daten können nur bei Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, oder bei bestimmten Straftaten in Verbindung mit Cyberkriminalität, Kinderpornografie, Fälschung im Zusammenhang mit unbaren Zahlungsmitteln oder Terrorismus angefordert werden.

Die bisher üblichen Rechtshilfegesuche zwischen den Mitgliedstaaten werden danach nicht mehr erforderlich sein. Die Behörden im Land des Online-Dienstes müssen nach Inkrafttreten der neuen Regelung nicht mehr benachrichtigt werden, wenn eine „Sicherungsanordnung" das Einfrieren von Daten für bis zu 60 Tage anordnet, auch dann nicht, wenn mittels einer Herausgabeanordnung Verkehrsdaten wie unter anderem IP-Adressen, angewählte Rufnummern oder auch Bestandsdaten angefragt werden, um die Identität von Nutzern festzustellen.

Behörden, die sensible Daten anfordern (z.B. Inhaltsdaten und Verkehrsdaten, die nicht nur zur Identifizierung verwendet werden), müssen die Behörden des Ziellandes benachrichtigen. Die benachrichtigte Behörde hat dann 10 Tage Zeit, die Anfrage zu überprüfen und gegebenenfalls Widerspruch einzulegen, wenn die Anfrage den Vorgaben des Gesetzes nicht genügt. Reagiert sie innerhalb dieser Frist nicht, muss der Diensteanbieter die Daten übermitteln. Bei grundrechtlichen Bedenken können die benachrichtigten Behörden dann Beweisanfragen an Dienstleister in ihrem Land auch ablehnen. Diensteanbieter selbst können ebenfalls rechtliche Bedenken gegen Anfragen äußern.

Die begleitende Richtlinie über gesetzliche Vertreter verpflichtet Unternehmen, die in der EU Dienstleistungen anbieten, Niederlassungen oder rechtliche Vertreter in der EU zu benennen, an welche die Behörden der Mitgliedstaaten Anfragen zur Übermittlung elektronischer Beweismittel richten können.

Eine weitere erhebliche Neuerung, neben der Tatsache, dass die üblichen Rechtshilfegesuche nicht mehr nötig sind, birgt ein erhebliches Konfliktpotential mit Drittstaaten: Nach der neuen Verordnung ist es irrelevant, wo die Daten, die im Rahmen einer Europäischen Herausgabeanordnung zu übermitteln sind, tatsächlich gespeichert sind: Dies kann der Fall sein a) in dem Staat, in dem der benannte Vertreter sitzt, b) in einem anderen EU-Staat, aber eben auch c) in einem Drittstaat außerhalb der Europäischen Union. Dass die Verpflichtung zur Herausgabe unabhängig vom Datenspeicherort gilt, ergibt sich aus verschiedenen Regelungen der Verordnung.[10] Damit Anordnungen an die Diensteanbieter adressiert werden können, ist es lediglich relevant, dass das jeweilige Unternehmen seine Dienste in der Europäischen Union anbietet, was insbesondere auf die großen Unternehmen aus den USA zutrifft. US-Diensteanbietern ist es aber grundsätzlich verboten, Inhaltsdaten, die auf Servern in den USA gespeichert sind, an ausländische Strafverfolgungsbehörden herauszugeben (18 U.S.C. § 2702). Die US-Diensteanbieter könnten dann zwar nach Art. 17 VO als Adressaten von Herausgabeanordnungen von der Möglichkeit Gebrauch machen, einen „Einwand" gegen die Herausgabeanordnung zu erheben. Soweit die Anordnungsbehörde die Anordnung aufrechterhalten will, entscheidet nach Art. 17 Abs. 3 VO ein Gericht des Anordnungsstaates anhand einer umfangreichen Abwägung, deren Wertungen sich aus einem ausführlichen Kriterienkatalog (Art. 17 Abs. 6 VO) ergeben, darüber, ob die Anordnung dennoch aufrechtzuerhalten ist: In die Abwägung ist etwa das Datenschutzinteresse des anderen Staates bzw. des die Herausgabe verhindernden Staates sowie der Grad der Verbindung der Strafsache mit der Europäischen Union zu berücksichtigen. Schon 2019 wurde die Europäische Kommission daher damit beauftragt, ein Abkommen zwischen der Europäischen Union und den USA über digitale Beweise auszuhandeln. Ziel aus EU-Sicht ist dabei,

dass das US-Datenschutzrecht es den US-Diensteanbietern nicht mehr verbietet, Europäischen Herausgabeanordnungen, die sich auf in den USA gespeicherte Daten beziehen, nachzukommen. Auf der anderen Seite möchten auch die Regierungsvertreter:innen aus den USA verhindern, dass sich die US-Diensteanbieter gegenüber US-Anordnungen nach dem sog. US CLOUD Act[11] zur Herausgabe von Daten, die auf Servern in der Europäischen Union gespeichert sind, auf das EU-Datenschutzrecht und dabei insbesondere die Art. 44 ff. DSGVO berufen dürfen. Danach ist die Herausgabe von in der EU verarbeiteten Daten ohne ein Abkommen zwischen der Europäischen Union und dem jeweiligen Drittstaat, an den die Daten übermittelt werden sollen, grundsätzlich verboten. Geregelt werden soll daher die Geltung der E-Evidence-Verordnung für US-Diensteanbieter auf der einen und der Zugriff der US-Ermittler:innen auf in der Europäischen Union gespeicherte Daten auf der anderen Seite.[12]

Nachdem die Verhandlungen lange ausgesetzt waren, wurden sie im März 2023 aus Anlass der bevorstehenden Verabschiedung des E-Evidence-Gesetzespakets wieder aufgenommen. Nach einer am 21. Juni 2023 veröffentlichten gemeinsamen Erklärung der EU- und US-Innen- und Justizminister:innen soll zur Sicherstellung von hinreichenden Verfahrens- und Grundrechten eine im vergangenen Jahr auf OECD-Ebene verabschiedete Erklärung als eine Grundlage für das E-Evidence-Übereinkommen dienen. Durch diese Erklärung werden bestimmte Mindeststandards festgeschrieben, etwa, dass es für den Zugriff auf Daten einer rechtlichen Grundlage bedarf und ein solcher nur für legitime Zwecke zulässig ist. Außerdem wird ein Gebot der Zweckbindung formuliert sowie ein gewisses Maß an Transparenz vorgegeben. Angesichts der vagen Formulierungen erscheint es jedoch fraglich, ob hierdurch den Art. 44 ff. DSGVO hinreichend Rechnung getragen wird.[13]

## IV. Zweites Zusatzprotokoll zur Cybercrime-Konvention des Europarates

Der Europarat hat am 17. November 2021 ein zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität angenommen. Es enthält Bestimmungen für eine effizientere Rechtshilferegelung, Bestimmungen über die direkte Zusammenarbeit mit Diensteanbietern in anderen Ländern, die Vertragsparteien des Übereinkommens sind, und einen Rahmen und Garantien für die Ausweitung grenzüberschreitender Abfragen. Das Protokoll enthält strikte Garantien und Datenschutzanforderungen. Da nur Staaten Vertragsparteien sein können, konnte die EU das Protokoll nicht unterzeichnen oder ratifizieren. Aus diesem Grund wurden die Mitgliedstaaten von der EU am 5. April 2022 zur Unterzeichnung und am 14. Februar 2023 zur Ratifizierung des Protokolls ermächtigt.

Ziel des Zusatzprotokolls ist die Ergänzung der Cybercrime-Konvention und ihres ersten Zusatzprotokolls. Der Anwendungsbereich umfasst jegliches elektronische Beweismaterial.

Auch für Verkehrsdaten ist lediglich ein beschleunigtes Rechtshilfeverfahren in Art. 8 des zweiten Zusatzprotokolls geregelt. Gem. Art. 8 können die Behörden einer Vertragspartei die Behörden einer anderen Vertragspartei um Übermittlung von Bestands- und Verbindungs-/Verkehrsdaten ersuchen. Art. 8 Abs. 6 gibt konkrete Fristen für die Weiterleitung der Anfrage an Diensteanbieter vor (45 Tage) sowie für die Beantwortung durch die Diensteanbieter (20 bzw. 45 Tage).

Für den grenzüberschreitenden Zugang zu Inhaltsdaten bei Telekommunikations- und Telemedienprovidern enthält Art. 9 einen beschleunigten Weg der Rechtshilfe über die nationalen Kontaktstellen des sog. 24/7-Netzwerks nach Art. 35.

Ein Direktzugriff ist im zweiten Zusatzprotokoll nur für Bestandsdaten im Sinne von Art. 18 Abs. 3 des Übereinkommens über Computerkriminalität (siehe Art. 7 des zweiten Zusatzprotokolls) und für Informationen bezüglich der Registrierung von Domänennamen im Internet (siehe Art. 6 des zweiten Zusatzprotokolls – auch hierbei handelt es sich der Sache nach um Bestandsdaten des Domain-Inhabers) vorgesehen.[14]

## V. UN-Cybercrime-Konvention

Während die USA und ihre Verbündeten der Auffassung sind, dass die Budapester Konvention das beste Abkommen ist, um Cybercrime zu bekämpfen, argumentieren Russland, China und viele Entwicklungsländer, dass die Budapester Konvention nur eine begrenzte Anzahl von Staaten repräsentiere und weit von einem globalen Konsens entfernt sei. Ein solcher könne nur auf der Ebene der UN erreicht werden.[15]

Nachdem Ansätze zur Aufnahme von Verhandlungen über eine UN-Cybercrime-Konvention immer wieder scheiterten, nicht zuletzt aufgrund der Intervention des Europarates bzw. einiger Mitgliedstaaten des Europarates, beschloss die UN-Generalversammlung am 27. Dezember 2019, ein Ad-hoc-Komitee zur Erarbeitung einer umfassenden Konvention zum Thema Cybercrime zu schaffen.

Die ersten fünf Treffen des Ad-Hoc-Komitees fanden 2021 und 2022 in Wien und New York statt. Am 26. Mai 2021 be-

schloss die UN-Generalversammlung bereits erste Details der Konvention. Die Generalversammlung regte eine breite Beteiligung von Nichtregierungsorganisationen an und betonte sowohl die Prinzipien der Transparenz als auch die geografische Ausgewogenheit und Geschlechterparität ausdrücklich.[16] Nach weiteren Treffen in diesem Jahr wird mit einer Verabschiedung der UN-Cybercrime-Konvention Anfang 2024 gerechnet.[17]

Eine erste veröffentlichte Gliederung der Konvention zeigt, dass folgende Kapitel vorgesehen sind: Grundsätzliche Vorschriften, Strafbarkeit, Prozessrecht, Internationale Zusammenarbeit, Technische Unterstützung, Prävention, Implementierung und Schlussbestimmungen. Da vor allem Russland und China brisante Vorschläge eingebracht haben, ist eine Debatte entbrannt. Ein russischer Vorschlag sieht unter anderem eine Pflicht für Provider vor, Strafverfolgungsbehörden weltweit beim Abhören in Echtzeit zu unterstützen, *„subversive oder bewaffnete Aktivitäten, die auf den gewaltsamen Sturz des Regimes eines anderen Staates gerichtet sind",* sollen verboten werden.[18] Das Verbreiten terroristischer und extremistischer Inhalte inklusive „politischer Hassrede" soll nach dem Willen Russlands global strafbar werden.[19] NGOs kritisieren insbesondere die in Art. 46 IV geregelten Verpflichtungen gegenüber Dritten, wie z.B. Diensteanbietern, entweder Sicherheitslücken in bestimmter Software offenzulegen oder den zuständigen Behörden Zugang zu verschlüsselter Kommunikation zu gewähren. Widerspruch regt sich auch gegen die in Art. 47 geregelte Erhebung von Verkehrsdaten in Echtzeit.[20] Mehr als 80 NGOs fordern, die UN solle dafür Sorge tragen, dass die Konvention „nicht das Hacken von Netzwerken und Endgeräten" ermöglicht.[21]. Das Abkommen habe das Potenzial, Millionen von Menschen auf der ganzen Welt tiefgreifend zu beeinflussen. Es müsse daher deutlich gemacht werden, dass der Kampf gegen die globale Cyberkriminalität nicht die Menschenrechte gefährdet oder untergräbt.[22]

## VI. Fazit

Der schnelle grenzüberschreitende Zugang zu digitalem Beweismaterial ist von entscheidender Bedeutung für eine erfolgreiche Bekämpfung der Cyberkriminalität. Zugleich gilt es hier, den Grundrechtsschutz und die staatliche Souveränität der betroffenen Staaten zu respektieren.

Während eine Überdehnung der existierenden strafprozessualen Befugnisse nicht zur Lösung beitragen kann, dürfte künftig die schnellste Lösung in der Anwendung des E-Evidence-Gesetzespakets der EU liegen. Vorausgesetzt ist freilich, dass die erwähnten noch notwendigen Verhandlungen mit den USA erfolgreich abgeschlossen werden. Das EU-Gesetzespaket tritt allerdings erst in drei Jahren in Kraft.

Eine deutliche Beschleunigung der Verfahren dürfte auch bei einer Ratifizierung des zweiten Zusatzprotokolls zum Übereinkommen über Computerkriminalität des Europarates erfolgen. Dieses Zusatzprotokoll wurde bisher von 42 Staaten unterzeichnet; 2 davon haben es ratifiziert. Deutschland hat es am 27. Januar 2023 unterzeichnet, jedoch bis dato noch nicht ratifiziert.

Mit Inkrafttreten der UN-Cybercrime-Konvention, sofern sie, wie angekündigt, im nächsten Jahr verabschiedet wird, wird es zwei Konventionen zu demselben Thema geben, sodass über die jeweilige Anwendung gem. Art. 30 des Wiener Übereinkommens über das Recht der Verträge zu entscheiden wäre. Es besteht hier die Gefahr, dass das Vorhandensein zweier allgemeiner Rechtsrahmen für ein und dasselbe Thema nicht zur Vereinfachung der Rechtshilfe zwischen den Staaten beitragen wird. Positiv ausgewirkt hat sich hier bisher die breite Beteiligung der NGOs an den Verhandlungen zur UN-Cybercrime-Konvention, welche zu einer notwendigen und breiteren Debatte in der Öffentlichkeit über die hier betroffene Souveränität der Staaten und den Grundrechtsschutz der Bürger:innen geführt hat.

1 Angaben des Europäischen Rates <https://www.consilium.europa.eu/de/policies/e-evidence/> (Zugriff: 15.9.2023).
2 Keyser, Journal of Transnational Law & Policy Vol. 12 (2), 289; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension, in: Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, S. 1 ff.
3 Angaben des Europäischen Rates <https://www.consilium.europa.eu/de/policies/e-evidence/> (Zugriff: 15.9.2023).
4 Dazu Gercke, ZUM 2022, 893.
5 LG Koblenz, Beschluss vom 24.8.2021 – 4 Qs 59/21.
6 LG Koblenz, a.a.O.
7 Bechtel, Anmerkung zu LG Koblenz vom 24.8.2021 – 4 Qs 59/21, NZWiSt 2022, 160, 162 ff.; Gercke, ZUM 2022, 893; Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, S. 371 f.; Bär ZIS 2011, 54; ders. Handbuch der EDV-Beweissicherung, 2007, Rn. 372 ff. insbes. 375; Hilbert/Trüg/Mansdörfer, Handbuch Cloud Computing, 2014, S. 559 f.; Borges/Meents/Gercke, Cloud Computing, 2016, Kap. 8 Rn. 40; Hegemann, BeckOK StPO, 44. Ed. Stand: 1.7.2022, StPO § 110 Rn. 14 mwN.
8 Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren, ABl L 191, 28.7.2023, 118.
9 Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die

**Professor Dr. Kristin Pfeffer**
Hochschule der Akademie der Polizei Hamburg, University of Applied Police Sciences, Forschungsstelle für Deutsches und Europäisches Sicherheitsrecht (FEDS)

Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren, ABl L 191, 28.7.2023, 181.
10 Art. 1 Uabs. 1 , Art. 17 Abs. 2 lit. b, Erwägungsgrund 21 der VO 2023/1543.
11 „Clarifying Lawful Overseas Use of Data Act (CLOUD Act)" <https://www.justice.gov/criminal-oia/page/file/1152896/download> (Zugriff: 15.9.2023). Dazu J. Daskal, "Unpacking the CLOUD Act", eucrim 2018, 220.
12 Zum Ganzen Meißner, Digitale Beweise im EU-/US-Datenschutzkonflikt, VerfBlog, 2023/6/28, <https://verfassungsblog.de/digitale-beweise-imeu-us-datenschutzkonflikt/> (Zugriff: 15.9.2023).
13 Meißner, aaO.
14 MüKo StPO/Rückert, 2. Aufl. 2023, § 100a StPO Rn. 46a.
15 Segura-Serrano, ZaöRV 2021, 701 ff.
16 Dazu Gercke, ZUM 2022, 893.
17 So Human Rights Watch, „Opening Stages in UN Cybercrime Treaty Talks Reflect Human Rights", 28. April 2022, <https://www.hrw.org/news/2022/04/28/opening-stages-un-cybercrime-treaty-talks-reflect-human-rights-risks> (Zugriff: 15.9.2023).
18 Art. 26 Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, A/AC.291/16, 7. November 2022, Englische Version, <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/A_AC291_16_Advance_Copy.pdf> (Zugriff: 28.09.2023).
19 Art. 27, a.a.O.
20 Offener Brief von mehr als 80 NGOs „Civil Society Letter on the Proposed Cybercrime Treaty", <https://epicenter.works/sites/default/files/cndletter-14.12.2022_0.pdf> (Zugriff: 15.9.2023).
21 Electronic Frontier Foundation (EFF), "Global Cybercrime and Government Access to User Data Across Borders: 2022 in Review", 2. Januar 2023, <https://www.eff.org/de/deeplinks/2022/12/global-cybercrime-and-government-access-user-data-across-borders-2022-year-review> (Zugriff: 15.9.2023).
22 Offener Brief von mehr als 80 NGOs, a.a.O (N. 20).

# The E-evidence Package

## The Happy Ending of a Long Negotiation Saga

Gianluca Forlani*

**The following article gives an overview of the long internal negotiations on the EU legal instruments aiming at improving cross-border access to e-evidence in judicial proceedings (the so-called e-evidence package), which have finally been concluded. It outlines the main challenges met during the negotiations and how they were overcome to reach a compromise which has become subject to political agreement. This compromise is expected to prove more useful from a practical point of view than previous, more general cooperation tools. In addition, the article puts the EU's legislative initiative into the context of legal instruments and negotiations on law enforcement access to e-evidence at the international level before turning to expected future developments.**

### I. Introduction

Legislative initiatives on e-evidence were presented more than five years ago. After conducting an in-depth assessment and following bilateral discussions with the delegations of the EU Member States, the European Commission published two proposals on 17 April 2018:

- A proposal for a Regulation on the European orders for the production and preservation of electronic evidence in criminal matters;
- A proposal for a Directive establishing harmonised rules on the appointment of legal representatives for the purpose of obtaining evidence in criminal proceedings.

These instruments and the ensuing negotiations faced several complex challenges. One of the main challenges was striking a fair balance between the fundamental rights related to the protection of privacy and the rights of suspects and accused persons on the one hand, and enabling/facilitating investigations and prosecutions of crime on the other.

While even with traditional judicial cooperation instruments, this balance is always difficult to strike, the specific case of e-evidence encountered a further obstacle: the need for a direct relationship between the judicial authority of a prosecuting state (issuing state) and a (private) entity outside its jurisdiction, i.e. a service provider who holds data that may include traces of communications and activities of perpetrators who operate through IT means. Thus, this "e-evidence scenario" deviates from the traditional trilateral relationship on the basis of mechanisms of letters rogatory that require the involvement of the judicial authority of the state where the service provider is located. This resulted in the fundamental question to which extent the judicial authority in the service provider state was to actively be involved . Should the latter simply be obliged to execute the order of the issuing judicial authority? Should it verify the correctness of the activity carried out by the issuing authority? In short, the e-evidence package was a real litmus test for the principles of mutual trust and mutual recognition that kept being invoked and flaunted throughout the negotiations. This raised the more general question of whether "mutual trust" means "blind faith" or "reasoned trust".

The following section (II.) outlines the background of the internal EU legislative rules on e-evidence and critical issues that emerged during the negotiations; this culminated in the provisional agreement of 25 January 2023 and – after linguistic and technical revision – the final texts that were signed on 12 July 2023 and published in the Official Journal of the European Union on 28 July 2023. However, the EU's e-evidence package must also be seen in the context of the overall legal framework on e-evidence at the international level (comprised of the Council of Europe Second Additional Protocol to the Cybercrime Convention, the bilateral negotiations on an EU-US e-evidence agreement, and the starting negotiations on a United Nations legal instrument on cybercrime), to which Section III. is dedicated. Section IV. of this article provides a brief outlook to the next steps of the EU dossier before additional and concluding remarks (Section V.).

## II. Background and Negotiations of the EU Legal E-evidence Package

### 1. Challenges/issues of electronic evidence acquisition in the current legal framework

Prior to the new e-evidence package, multiple international cooperation instruments had been used under the EU legal framework for cross-border electronic evidence gathering. These instruments include:

- Directive 2014/41/EU on the European Investigation Order in criminal matters (EIO);
- The European Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union;
- Regulation (EU) 2018/1727 of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust);
- Regulation (EU) 2016/794 on Europol;
- Council Framework Decision 2002/465/JHA on joint investigation teams;
- Bilateral agreements between the Union and third states, such as the mutual legal assistance agreements in force with the US;
- The Council of Europe Convention on Cybercrime (Budapest Convention).

Yet in practice, these comprehensive and wide-ranging legal cooperation instruments have still failed to adequately address some of the difficulties encountered in the process of obtaining electronic data. One of the most significant obstacles in this context has been the refusal by Internet service providers to make data available in cases where the authority in question lacks jurisdiction over the place of the establishment of its headquarters, or because of the nationality of the affected person for whom data has been requested. More complex problems arise when a case is connected with the legal system of states outside the EU (third states), which is a recurring scenario given that the largest providers of telematic services are based in the United States. In addition to the aforementioned jurisdictional problems, obtaining electronic evidence through judicial cooperation procedures – whether conventional or based on the principle of mutual recognition – has always necessitated the involvement of the (judicial and/or governmental) authority of the executing/requested state. This inevitably causes delays, which is clearly incompatible with the "volatility" of electronic data.

### 2. The Commission's two regulatory proposals

With the two proposals listed earlier, the Commission intended to overcome these shortcomings. Notwithstanding this ambition, they are designed to complement, and not replace, existing judicial cooperation instruments, in particular the EIO. The Regulation aims to simplify and accelerate the process of securing and obtaining electronic evidence stored and/or held by service providers established in another jurisdiction. This objective is to be achieved by directly transmitting the order to preserve/produce data to the representative designated by the service provider, with

the latter being obliged to comply by directly handing over the data to the requesting authority. This obligation applies unless there are specific and compelling reasons not to do so, and without being able to oppose reasons related to the place where the data are stored. In turn, the corresponding Directive aims to establish an obligation for service providers offering their services in the EU to designate a legal representative in at least one Member State.

It follows that the relevant procedural mechanisms need to be structured according to general models to make them useful from an operational point of view and ultimately ensure their practical applicability. In other words, the negotiations made it clear that unless speed and efficiency are to be improved with a new European production order, the prosecuting authorities would continue to use the cooperation tools already available.

## 3. Critical pre-trilogue issues emerged in the Council

Negotiations on the two proposals started in the COPEN Technical Working Group on 27 April 2018 under the Bulgarian Council presidency, and continued under the subsequent Council presidencies. From the outset, the process placed great emphasis on working around the principle of territoriality in the traditional sense, which was achieved by declaring the location of the data to be irrelevant. However, some technical issues immediately emerged as harbingers of several other critical points. These included:

- Potential conflicts with obligations under the law of third countries (and, in this context, the relationship between the proposed new instrument and the US CLOUD Act);
- A possible extension of the subject matter of the Regulation to include direct access to data by authorities and real-time interceptions, which are considered to be extremely relevant investigative tools;
- The question of whether orders should also be served to the relevant authority of the executing state or of another state that has a connection with the case at issue.

The Austrian Council presidency presented a compromise text (which reflected the negotiating efforts of the Member States to reach an agreement) to the Justice and Home Affairs (JHA) Council in December 2018. At this meeting, the Council's general approach on the draft Regulation was adopted while that on the draft Directive was reached in the JHA Council in March 2019. While the Member States supported the compromise text of the Austrian presidency, some called for subtle changes. For example, two states suggested introducing a more incisive procedure of notifying authorities in the affected persons' states; others would have preferred a more streamlined procedure that would have seen no other authorities or states notified at all.

## 4. Pre-trilogue contributions by other institutions

The European Economic and Social Committee adopted its opinion as early as on 12 July 2018. Conversely, the European Parliament (EP) as co-legislator appointed its rapporteur on 24 May 2018. Subsequently, several meetings and hearings were held in the LIBE Committee on the e-evidence proposal, including a public hearing on 27 November 2018.

The LIBE Committee developed amendments to numerous key provisions of the regulation, being in strong contrast with the Council's general approach. The Committee, *inter alia*, proposed replacing the Directive and integrating some of its provisions into the Regulation (a solution that casted serious doubts on the appropriateness of the latter's legal basis). The large number of proposed amendments tabled by the parliamentary political groups, together with the onset of the pandemic, further slowed down work on a final EP position, which was finally adopted as late as in mid-December 2020. The EP's text was still far from the one that the Council had drafted in its general approach. The EP followed a much more restrictive approach on central issues, such as:

- The prerequisites for issuing orders (three additional prerequisites were inserted);
- The need for notification to the executing state with substantial effects for all orders and for all types of data;
- The extension of the grounds for refusal and the inclusion of mandatory ones;
- The merger of the Directive with the Regulation.

A rather carefully-worded position was also expressed by the European Data Protection Supervisor (EDPS) on 6 November 2019. On the one hand, the EDPS supported in his opinion "the objective of ensuring that effective tools are available to law enforcement authorities to investigate and prosecute criminal offences, and in particular welcomed "the objective of the Proposals to accelerate and facilitate access to data in cross-border cases by streamlining procedures within the EU." On the other hand, the EDPS underlined "that any initiative in this field must be fully respectful of the Charter of Fundamental Rights of the EU and the EU data protection framework…" The EDPS advocated for a greater involvement of judicial authorities in the enforcing Member States and expressed a wish for them to be "systematically involved as early as possible in this process" in order to "have the possibility to review compliance of orders with the Charter and have the obli-

gation to raise grounds for refusal on that basis." In addition, the EDPS voiced the need to clarify the definitions of data categories in order to make them consistent with other definitions of data categories in EU law. He eventually recommended "reassessing the balance between the types of offences for which European Production Orders could be issued and the categories of data concerned in view of the relevant case law of the Court of Justice of the EU."

## 5. The trilogue negotiations and compromise

The inter-institutional negotiations between the Commission, the Council, and the European Parliament (the so-called trilogue) started in January 2021 under the Portuguese Council presidency. The trilogue negotiations spanned four further Council presidencies (Slovenia, France, the Czech Republic, and Sweden). At the beginning of 2023, a compromise was found under the Swedish presidency.

Trilogue turned out to be particularly complex due to the profound differences between the text of the Council's general approach and the EP's position. The EP advocated a much more restrictive instrument, having proposed to introduce a greater number of prerequisites for orders by the issuing authority and a generalised regime of notification to the state of execution covering all orders and all types of data with substantial effects. This was accompanied by an extensive list of grounds for refusal, some of which were considered mandatory. Moreover, the EP proposed abandoning the Directive, incorporating some of its provisions into the Regulation (cf. above 4.).

On the part of the Council, diverging views emerged: Some more ambitious delegations supported the solution proposed in the general approach, considering it suitable to guaranteeing an adequate level of effectiveness of the instrument and at the same time high standards of protection of fundamental rights; yet other delegations reiterated their general support for a stronger and more extensive notification regime, while considering some options of the EP to be overly restrictive. In the absence of any obvious willingness to compromise on the part of the EP's negotiators, the Council conducted the negotiations by sticking as closely as possible to the text of the general approach during this initial phase.

Given the EP's persistence on its position, the Council adopted a different approach in the second half of 2021 and suggested compromise solutions, showing some flexibility with respect to its general approach. Such solutions included, for instance, the suggestion that all forms of notification for preservation and production orders related to subscribers' data and so-called identification data (traffic data used solely for identification purposes, such as IP addresses, ports, etc.) be removed. In addition, no notification was to be needed for production orders of traffic data belonging to subjects residing in the issuing state, whereby such residence was to be presumed unless there were reasonable grounds to believe otherwise.

Even though this compromise solution was supported by the Member States (primarily as *ultima ratio* in order to break the deadlock), the EP found it insufficient in view of fundamental rights concerns.

Nevertheless, the Council continued its efforts to reach a final agreement on the instruments by tabling new compromise texts. In particular, issues not related to notification (on which a preliminary agreement had not yet been reached between the co-legislators) were brought back to the negotiating table. The discussion on the proposal for a Directive on harmonised rules for the appointment of legal representatives for the purpose of obtaining evidence in criminal proceedings, previously shelved as particularly controversial, was reopened. The debate on the Directive was fruitful, with the EP accepting to maintain the Directive as a separate instrument and as a way of settling good compromise solutions on almost all outstanding issues.

At the same time, the Council drew up a compromise proposal. While still aiming to uphold the residence criterion for both content and traffic data, it included some key points of the EP position, such as a single regime for content and traffic data, notification with suspensive effect, and a list of grounds for non-execution, including at least immunities and privileges, fundamental interests and security of the executing state, freedom of the press and freedom of expression, and fundamental rights. The proposal was supported by the majority of Member States, but attempts to reach an agreement with the EP were unsuccessful.

Following a deadlock, the dialogue between the EP and the Council resumed in May 2022. Despite significant disagreement on crucial issues (notification, grounds for refusal, residence criterion), intense negotiating efforts by the parties allowed them to make good progress in bilateral discussions. At the end of 2022, attempts were intensified to finally reach an agreement, in line with the Commission's position. At the meeting of the Permanent Representatives Committee on 23 November 2022, the Council presidency asked the Member States to be granted a mandate for the trilogue meeting on 29 November to present an overall compromise package. This package, which was finally

agreed on by both the Member State delegations and the EP, included the following:

- Application of the residence criterion to exclude notification to the executing state: Due to the burden of proof of residence being reversed and put on the issuing authority, the EP insisted on setting a number of requirements for proof of residence (e.g. proof by way of an identity document or entry in a public register, a minimum period of residence, and other circumstances that were considered to be mandatory). In practice, this makes such proof very difficult for the issuing authority. It was, however, agreed that said requirements were to be placed in a recital, with the understanding that they would be mere indicators that could be used to prove the stability of permanence in the territory of the issuing state, rather than representing necessary and prescriptive requirements.
- Refusal of orders as a consequence of a pending rule-of-law procedure under Art. 7(1) and (2) of the Treaty on European Union (TEU): The EP initially proposed inserting grounds for refusal that referred to a pending Article 7 TEU procedure against the issuing State dealing with serious violations of the values mentioned in Article 2 TEU into the operative part of the Regulation. This was moved to a recitaland rephrased to avoid any automatism.
- Optional nature of the grounds for refusal and limited role of the service provider in non-execution of orders: The final compromise provides that service providers may only put forward a limited number of refusal grounds. In addition, they are obliged to inform the issuing authority and, if notification is required, the enforcing authority before a possible non-execution. Since service providers are private entities, they are not entitled to refuse requests on the grounds of fundamental rights violations; such assessment is reserved to the discretionary power of the judicial authority of the service providers' location.
- The distinction between the service provider and the data controller: Where the data controller differs from the Internet service provider, the issuing authority has the general obligation to address the order to the controller; however, the issuing authority is granted extensive exceptions in order to not hamper or slow down the investigation.
- Deletion of data: The compromise includes an obligation to delete (or alternatively restrict the use of) data transmitted in response to orders issued in urgent cases in the absence of notification if grounds for refusal emerge after transmission. This was done in respect to the EP's initial demand that the issuing authority be obliged to delete data received in an emergency case as and when grounds for refusal are raised.

## III. E-evidence for Criminal Proceedings: the International Context

The important step forward achieved with the EU's internal rules on access to e-evidence by the EU's judicial authorities also needs to be assessed against the background of parallel international legal instruments (existing and planned). The EU legal framework is a central starting point for negotiations on the same topic undertaken by the EU with third countries. At the same time, the new EU system constitutes an essential benchmark for verifying the consistency of other systems with the fundamental rights touched by the search and acquisition of electronic evidence, bearing in mind that it is subject to the case law of the Court of Justice of the European Union (CJEU) and, more broadly, of the European Court of Human Rights (ECtHR).

During the JHA Council meeting held on 6–7 June 2019, the justice ministers of the EU Member States approved the *Council Decision authorizing the European Commission to initiate negotiations with the United States regarding cross-border access to electronic evidence in the context of judicial cooperation in criminal matters* and the addendum containing the relevant negotiating directives. However, this dialogue with the US has been suspended pending the prior conclusion of the EU internal rules. It is now about to be resumed as the EU e-evidence package has been agreed.

At the JHA Council meeting of June 2019, the ministers had also adopted the *Decision authorising the participation of the European Union in the negotiations for the adoption of a Second Protocol additional to the Budapest Convention on Cybercrime,* which handed the European Commission a mandate to represent the European Union at the Council of Europe (CoE) level. The Second Protocol was finalised in December 2021, and opened for signature on 12 May 2022 under the Italian presidency of the CoE. It will enter into force after ratification by at least five states. After consent by the EP on 17 January 2023, the Council adopted a decision on 14 February 2023 authorising the EU Member States to ratify the Second Protocol, in the interest of the EU. The Second Protocol provides tools to strengthen cooperation and dissemination of electronic evidence and includes the following main features:

- In principle, direct cooperation between competent authorities of CoE member states and service providers of another state party;
- Effective means of obtaining subscriber information and traffic data;

- Obligation to create specific channels for rapid and direct cooperation between state authorities and between these authorities and private entities established in the territory of another state party;
- Competent state authorities may request the information necessary to identify or contact the registrant of a domain name in possession or under the control of the provider from service providers established in the territory of another state party;
- Considering that the range of participants in the Budapest Convention is broader and less homogeneous than EU Member States, a state party can always claim the right to notification to filter out requests;
- State authorities may require a service provider established in the territory of another state party to disclose the information on a subscriber, in possession or control of the service provider, where the information is necessary for specific criminal investigations and proceedings;
- Detailed regulation of the content of the request and the time limit within which the order must be enforced. If a service provider does not disclose the requested information by the deadline or expressly refuses to provide it, the authorities of the requesting state may seek to enforce the order in accordance with the procedure set out in Art. 8;
- According to Art. 8, cooperation does not take place between the authority and the private service provider, but between the national authorities of the states concerned (requesting and requested): the requested state must make every reasonable effort to compel the service provider in its territory to disclose the subscriber information and traffic data as quickly as possible or, in any case, within the time limits laid down in the Budapest Convention;
- Establishment of a cooperation scheme in emergency cases to obtain data stored by a service provider, including accelerated communication channels;
- Possibility for two or more State parties to allow their competent authorities, on the basis of mutual agreements, to establish and operate a joint investigation team in their territories to facilitate criminal investigations or proceedings (where enhanced coordination is deemed to be of particular utility);
- Clarification that other bilateral or multilateral agreements regulating the exchange of e-evidence are applicable, including the EU e-evidence Regulation (and the corresponding Directive) as well as any future agreements between the EU and the US.

Efforts to regulate e-evidence are also ongoing at the United Nations level. Through its Resolution 74/247 adopted on 27 December 2019, *Countering the use of information and communications technologies for criminal purposes,* the UN General Assembly established an Intergovernmental Committee of Experts (Ad Hoc Committee) with representatives from all UN countries to draft a global Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. The first negotiating session of the Committee took place in New York from 28 February to 11 March 2022. The General Assembly decided, *inter alia,* that the Ad Hoc Committee should convene at least six sessions of ten days each, followed by a concluding session in New York. The sixth session took place in New York from 21 August to 1 September 2023 and a concluding session is scheduled to take place in New York between 29 January and 9 February 2024. The EU also participates in the negotiation as an observer. Even though it is premature to predict the final outcome, the EU Member States' approach should be not to exceed the scope of the Second Protocol to the CoE Budapest Convention.

## IV. Towards Adoption of the EU Legal Instruments – Next Steps

The e-evidence Regulation entered into force on 18 August 2023 and it will apply from 18 August 2026 (Art. 34 of the Regulation). According to Art. 33 of the Regulation, the Commission shall carry out an evaluation of it by 18 August 2029 (six years from the entry into force of the Regulation). The Commission shall transmit an evaluation report to the European Parliament, the Council, the European Data Protection Supervisor, and the European Union Agency for Fundamental Rights. This evaluation report should include an assessment of the application of the Regulation and of the results that have been achieved with regard to its objectives, and an assessment of the Regulation's impact on fundamental rights. The evaluation should be conducted in accordance with the Commission's better regulation guidelines.

As far as the Directive is concerned, Art. 7 provides that Member States must bring into force the laws, regulations and administrative provisions necessary to comply with it by 18 February 2025. The discrepancy between the date when the Regulation will become applicable in the Member States and the date to bring into force the laws, regulations, and administrative provisions necessary to comply with the Directive is obviously linked to the fact that the Directive is a necessary precondition to the Regulation. Art. 8 of the Directive provides for the Commission to carry out its evaluation by 18 August 2029, i.e., in parallel with the one of the Regulation.

## V. Additional Remarks and Conclusion

Considering the relevance of electronic data as evidence, the agreement on the e-evidence package represents the achievement of a crucial tool in view of future developments in judicial cooperation in criminal matters. The most noticeable innovations of the e-evidence package concern, on the one hand, the irrelevance of the location of the data, and, on the other hand, the attempt to provide for a direct relationship between the requesting state and the service provider, with the competent authority of the executing state intervening only when the provider does not comply within a set period of time.

Given the potentially high invasiveness of the measures in question, it is noteworthy that the EU e-evidence Regulation co00ntains a number of robust procedural safeguards, for example:

- Protecting personal data by referring to the applicability of the EU General Data Protection Regulation (GDPR) and the EU Data Protection Directive for police and justice activities;
- Providing grounds for refusal which the judicial authority of the state in which the service provider is located and who must be notified of the request for data may oppose to the requesting state, particularly to ensure the protection of fundamental rights;
- Distinguishing between the different types of data according to their intrusiveness and providing different guaranties with reference to the issuing authority: If subscriber data or data requested for the sole purpose of identifying a person (e.g., the owner of an e-mail address) are to be obtained, the order has to be issued by a judge or by a public prosecutor. If the data is considered more invasive (i.e., traffic or content data), a request by a judge is required;
- Requiring that production orders may be issued in criminal proceedings in which offences are prosecuted for which a minimum term of imprisonment of four months is prescribed for the aforementioned first type of data or three years for traffic or content data. In the latter case, the possibility of issuing the order in relation to a number of particularly serious offences (albeit with a lower sanction) is also provided for (i.e., fraud and counterfeiting of non-cash means of payment; sexual abuse and sexual exploitation of children and child pornography; attacks against information systems [all if they are wholly or partly committed by means of an information system] and terrorism offences);
- Providing time limits for the preservation of data until a subsequent request for production.

It should finally be stressed, however, that the legal e-evidence instruments presented above regulate the access and/or the acquisition of data as evidence, which means that they presuppose the existence of such data. They do not regulate obligations to retain data. The retention of data is equally important and is closely linked to the subject matter of e-evidence. Adequate regulation on data retention cannot be negated. Even "ordinary" criminal proceedings are notoriously time-consuming, not least to ensure that a fair trial and the rights of the suspects/accused persons are duly guaranteed. Moreover, a crime is often discovered only after a considerable period of time has elapsed since the commission of the offence. If data are not retained or are retained for a too short period in such cases, all the rules governing their acquisition risk finding limited application; they might even risk remaining a purely stylistic exercise. This implies the need for striking a good balance between the strictness of the rules governing access to data and the retention of data for an adequate period of time. The CJEU has reaffirmed its stance on data retention in various judgments and emphasised that interference entailed by the retention of traffic and location data is justified only to combat serious crime or to prevent serious threats to public security. It remains to be seen whether a very recent judgment (CJEU judgment of 7 September 2023 in *Lietuvos Respublikos generalinė prokuratūra)* will provide fresh impetus to the discussion on the limits to and concrete rules on data retention. After a first reading of the judgment, the CJEU provided not only interesting pointers to how the leeway to regulate data retention can be implemented in the various legal systems, but also provided guidance as to the relationship between different kinds of proceedings and the mutual use of retained data. This raises the interesting question of whether a dividing line should be drawn *a priori* between the different kinds of proceedings (administrative, criminal) with a prejudicial distinction of the value of the interests protected therein or whether the level of the interests at stake should be assessed from time to time with a view to enabling the use of retained data in other proceedings regardless of their nature. At the same time, the CJEU ruled on the procedural consequences if the conditions of the Union law on data retention are not met. Whereas previous case-law left this question open, the Court now expressly precludes the use of the data as evidence.

---

* The views expressed in this article are solely those of the author and are not an expression of the views of the institution he is affiliated with. The printing of this article does not include the full text of relevant recitals/legal provisions. They can be accessed in the online version of the article at < https://eucrim.eu/articles/>.

**Gianluca Forlani**
Judge, former JHA Counsellor – Judicial Cooperation in criminal matters, Permanent Representation of Italy to the European Union, Brussels

1 COM(2018) 225 final.
2 COM(2018) 226 final.
3 For a summary of the proposal, see also T. Wahl, "Commission Proposes Legislative Framework for E-evidence", (2018) *eucrim,* 35.
4 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *O.J.* L 191, 28.7.2023, 118–180; Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *O.J.* L 191, 28.7.2023, 181–190.
5 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *O.J.* L 130, 1.5.2014, 1; see also, inter alia, J.A. Espina Ramos, "The European Investigation Order and its Relationship with Other Judicial Cooperation Instruments", (2019) *eucrim,* 53.
6 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *O.J.* C 197, 12.7.2000, pp. 1 et seq.
7 Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, *O.J.* L 295, 21.11.2018, 138.
8 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *O.J.* L 135, 24.5.2016, 53.
9 Council Framework Decision of 13 June 2002 on joint investigation teams, *O. J.* L 162, 20.06.2002, 1.
10 Agreement on mutual legal assistance between the European Union and the United States of America, *O.J.* L 181, 19.7.2003, 34.
11 European Treaty Series No. 185.
12 In this regard, it should be pointed out that the new US legislation on matters of e-evidence, i.e., the CLOUD Act approved on 23 March 2018, obliges US service providers to comply with requests for data production (even if stored outside US territory and thus, hypothetically, also on EU territory) *only if they originate from US authorities*. By contrast, enforceable agreements between the respective foreign governments are required if data are to be delivered (even directly) to foreign authorities.
13 *Op. cit.* (n. 1 and 2).
14 Council of the EU, Press release of 7 December 2018: „Regulation on cross border access to e-evidence : Council agrees its position" <https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/> accessed 20.09.2023.
15 European Parliament Report - A9-0256/2020, <https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html>; for an interesting insight into the EP's position, see also E-Evidence Package - The Position of the European Parliament, Update 9/08/2021, <https://www.eurojust.europa.eu/sites/default/files/assets/e-evidence-package-the-position-of-the-european-parliament.pdf> accessed 20.09.2023.
16 Opinion 7/2019, available at: <https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf> accessed 20.09.2023.
17 The final compromise is reflected in Recitals 52 and 53 of the Regulation, *op. cit.* (n. 4).
18 Cf. recital no 64 of the Regulation.
19 Reflected in Recitals 56 to 59 and Arts. 10(2), 10(3) and 10(5) of the Regulation, *op. cit.* (n. 4).
20 The final compromise is reflected in Arts. 5(6) and 5(7) of the Regulation.
21 The final compromise is reflected in Arts. 4(5) and 10(4) of the Regulation.
22 See T. Wahl, "E-Evidence: Commission obtains Mandates for EU-US agreement and Negotiations in Council of Europe" (2019) *eucrim,* 113.
23 Ibid.
24 Council of the EU, Press release of 14 February 2023: "Access to e-evidence: Council authorises member states to ratify international agreement", <https://www.consilium.europa.eu/en/press/press-releases/2023/02/14/access-to-e-evidence-council-authorises-member-states-to-ratify-international-agreement/> accessed 20 September 2023.
25 Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence, Strasbourg, 12.V.2022, CETS No. 224.
26 Art. 6 of the Second Protocol.
27 Cf. Art. 7 para. 5 of the Second Protocol: "A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, notify the Secretary General of the Council of Europe that, when an order is issued under paragraph 1 to a service provider in its territory, the Party requires, in every case or in identified circumstances, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation or proceeding."
28 Art. 7 and 8 of the Second Protocol.
29 Arts. 9 and 10 of the Second Protocol.
30 Art. 12 of the Second Protocol.
31 Art. 15 of the Second Protocol.
32 *Op. cit.* (n. 4).
33 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* L 119, 4.5.2016, 1.
34 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *O.J.* L 119, 4.5.2016, 89.
35 Art. 4(1) and 4(2) of the Regulation.
36 Art. 11(1) of the Regulation.
37 *Inter alia:* judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland/Seitlinger et al.*); judgement of 21 December 2016, Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB/Watson et al.*); judgment of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and Others*); judgment of 5 April 2022).
38 Case C-162/22.

# The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice

## An Introduction to the New EU Package on E-evidence

Adam Juszczak & Elisa Sason*

**Digital technologies have advanced more rapidly than any other innovation in modern history and they permeate our daily lives. The benefits to our societies and economies are numerous, but the risks of cyberattacks and crime have also increased. The EU is committed to protecting its citizens against these risks in the Area of Freedom, Security and Justice. Prevention, detection, and enforcement form key components of the EU's security architecture. Making use of the benefits of digital technologies and ensuring a high level of security across the Union were driving forces behind the latest building block in this architecture: the e-evidence package. Recently adopted, it aims to ensure that judicial and law enforcement authorities can obtain electronic evidence across the EU and beyond in a swift and legally sound manner for the purpose of investigations and prosecutions in criminal cases.**

**This article provides an introduction to the two new EU instruments: the Regulation on European Production/Preservation Orders and the Directive on the designation of designated establishments and the appointment of legal representatives. The authors outline the key elements of this new set of rules and illustrate their implications for stakeholders. Furthermore, the borderless and open character of digital technology also makes it imperative to analyse existing and potential new international agreements in this field, since they will have an impact on the effectiveness of the enacted EU e-evidence package.**

**The article concludes that the adoption of the EU e-evidence rules is an important step in the joint efforts to fight crime effectively. Fundamentally relying on the principle of mutual trust among the EU Member States and a presumption of their compliance with Union law, the rule of law, and fundamental rights and values, the application of the e-evidence package will nonetheless require constant scrutiny, monitoring, and cooperation between all actors involved.**

### I. Introduction

While it is common knowledge that digitalisation brings numerous benefits to our societies and economies, criminals are massively (mis-)using digital technologies to plan and commit criminal offences. Ensuring a high level of cybersecurity for digital products and services and having in place adequate tools for law enforcement authorities to investigate and prosecute criminal offences are ultimately two sides of the same coin. Recent developments, such as the COVID-19 pandemic and Russia's war against Ukraine, reaffirm the need for the EU to protect its citizens against the exploitation of known and new vulnerabilities, in full respect of fundamental rights. Prevention, detection, and enforcement form key components of the EU's security architecture.[1]

In the aftermath of the 2016 terrorist attacks, the Council adopted conclusions on improving criminal justice in cyberspace.[2] In these conclusions, the Commission was requested *inter alia*

> to develop a common framework for cooperation with service providers for the purpose of obtaining specific categories of data, in particular subscriber data, when allowed by third countries legislation, or any other comparable solution that allows for a quick and lawful disclosure of such data" and "to find ways, in association with Member States and, where necessary, third countries, as a matter of priority, to secure and obtain e-evidence more quickly and effectively by streamlining the use of mutual legal assistance proceedings and, where applicable, mutual recognition.

Similarly, in its Resolution of 2017,[3] the European Parliament called on the Commission to put forward a European legal framework for e-evidence, noting that "a common European approach to criminal justice in cyberspace is a matter of priority, as it will improve the enforcement of the rule of law in cyberspace and facilitate the obtaining of e-evidence in criminal proceedings."

To ensure that judicial and law enforcement authorities can obtain electronic evidence across the EU and beyond in a swift and legally sound manner for the purpose of investigations and prosecutions in criminal cases, the Commission proposed on 17 April 2018 a legislative package[4] composed of a Regulation on European Production and Preservation Orders and a Directive on the appointment of legal representatives. According to the Commission, cross-border access to electronic evidence for criminal investiga-

tions is needed in 85% of investigations, with 65% of the total requests going to providers based in another jurisdiction.[5] The volatile nature of electronic evidence makes access by law enforcement authorities essential, particularly in view of presenting it as admissible evidence before courts. Compared to traditional mutual recognition instruments, the novelty of these proposals is that orders may be directly addressed to a representative of a service provider in another Member State, without the authority of that other Member State being systematically involved in the process.

Having an internal EU framework in place – ideally followed by its proper application in practice – is, however, not the end of the story. Ensuring coherence and consistency between the EU's e-evidence rules and international agreements already agreed or still under negotiation, such as the Second Additional Protocol to the Budapest Convention of the Council of Europe, the United Nations Cybercrime Convention, and the EU-U.S. e-evidence agreement, is pivotal for the legal certainty of all stakeholders affected by this newly adopted framework.

This article provides a short background on the negotiations concerning the e-evidence proposal package (section II), outlines the key elements of the enacted e-evidence package (section III), and illustrates the implications of the new set of rules for stakeholders (section IV). It also touches upon existing links with international agreements (section V) and ends with a number of concluding remarks (section VI).

## II. Negotiations and Adoption of the E-evidence Package

Following the adoption of the Commission's proposal in 2018, it took five years for co-legislators to agree on this package. The proposal was welcomed and garnered support for having in place faster tools for obtaining electronic evidence, but it also faced criticism in the form of warnings not to lower existing standards, particularly as regards the protection of fundamental rights.[6]

It is telling that seven Member States, including Germany and the Netherlands,[7] could not support the General Approach adopted by the Council in December 2018.[8] In addition, the high number of amendments proposed by the European Parliament – the Parliament put forward 841 amendments[9] – demonstrates the difficult path towards finding a compromise. The most contentious points of the negotiations were: the design of the notification mechanism, namely whether the authority of the Member State in which the service provider or legal representative is located should be involved in reviewing the Order; if so, for which type(s) of data; and whether the authority may assert grounds to refuse requests.

After eight trilogues, political agreement was reached in November 2022 and confirmed in Council (Coreper) and the European Parliament (LIBE Committee) in January 2023. The Regulation and Directive were published in the Official Journal on 28 July 2023.[10] While the Regulation will come to application 36 months after its date of entry into force, i.e., on 18 August 2026,[11] Member States will have 30 months to transpose the Directive after its entry into force, i.e., on 18 February 2026.[12] This allows Member States to make the necessary adaptations in their national laws and put everything in place before the e-evidence package starts to apply.[13]

## III. Key Elements of the Enacted E-evidence Package

With its new e-evidence package, the EU introduces an entirely new system of obtaining electronic evidence in criminal proceedings by directly addressing private providers of communication, data storage, and internet infrastructure services located in another Member State – without, in principle, the need to involve the national authorities of the Member State in which the service provider is located. Such an approach can only function properly on the basis of a high level of mutual trust between the Member States.[14]

The new EU package on e-evidence is built on two distinct pieces of legislation:

- Regulation (EU) 2023/1543 lays down the rules and safeguards for national authorities to order service providers located in another Member State to preserve and produce e-evidence for the purpose of carrying out criminal proceedings;
- Directive (EU) 2023/1544 sets out, by contrast, harmonised rules on the designation of designated establishments or legal representatives by the service providers in order to ensure receipt, compliance with, and enforcement of orders issued by the competent authorities in the Member States for the purpose of gathering electronic evidence under the Regulation.[15]

Both legal acts shall be described in the following subsections.

### 1. Regulation on E-evidence

The Regulation, which is based on Art. 82(1) of the Treaty on the Functioning of the European Union (TFEU), introduces two new central instruments applicable across the Union for

the purpose of obtaining electronic evidence in criminal proceedings – the European Production Order and the European Preservation Order. The choice of legal basis was subject to strong criticism but was not changed by the legislator.[16]

These instruments are defined as decisions issued or validated by the judicial authority of a Member State and addressed to a designated establishment or legal representative of a service provider offering services in the Union and located in another Member State for the purpose of producing electronic evidence or for preserving electronic evidence with a view of a subsequent request for production, respectively.[17] With the European Preservation Order, judicial authorities may prevent foreign service providers from deleting or altering data, while the European Production Order enables the authorities to request preserved information directly from the service providers immediately or at a later stage.

To this end, the Regulation governs the conditions for the issuing of these instruments, its execution by the service providers, notification of and grounds of refusal for the executing Member State, the enforcement and penalties procedure, rights of the persons whose data is sought, a review procedure in case there are conflicting obligations with laws of a third state, provisions on standardised certificates and a decentralised IT system, and lastly rules governing the costs.

The Regulation does not, however, provide for a complete and exhaustive set of rules governing the application of the European Production Order and the European Preservation Order but instead refers on numerous occasions to rules provided under national law.

### a) Subject matter and scope of the Regulation (Articles 1 and 2)

The material scope of application of the Regulation is limited to orders in the context of and for the purpose of criminal proceedings and for the execution of custodial sentences or detention orders of at least four months imposed by a decision not rendered *in absentia*. The orders may also be issued in criminal proceedings directed against a legal person. This means that these instruments cannot be used for preventive purposes or as a means of continuous surveillance. It requires the existence of concrete criminal proceedings, meaning that there is neither room for these instruments before criminal proceedings have commenced, nor once they have been terminated. Moreover, the Regulation also clarifies that it does not apply in mutual legal assistance proceedings, for which other respective instruments are to be used.

The Regulation defines the term "electronic evidence" as subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form,[18] i.e., emails, text messages or content from messaging apps, audio-visual content, or information about a user's online account. These categories of data correspond with the EU *acquis*[19] and established jurisprudence of the Court of Justice of the EU, as well as with the types of data used in the Member States and with international instruments.[20]

In terms of personal and territorial scope, the Regulation focuses on service providers offering services in the Union. The Regulation thereby targets service providers that provide electronic communication[21] and other information services[22] that enable users to communicate with each other or that process or store data on behalf of the users, such as telecom or social media companies. This includes voice-over IP, instant messaging, and email but also marketplaces and other hosting services as well as online gaming and gambling platforms.[23] Providers of internet infrastructure services, such as domain name registries, proxy service providers, and internet protocol registers, are also covered and of particular relevance, as they hold data that could allow for the identification of an individual or entity user or the victim of a criminal activity.[24]

The determination of whether a service provider is offering services in the Union is based on an assessment of two cumulative requirements. The first requirement concerns the availability of the services in a Member State, while the second requirement demands that there be a substantial connection, based on specific factual criteria, to that Member State or those Member States of the Union.[25] Such a substantial connection is considered to exist if the service provider has an establishment physically located in the Union. In the absence of an establishment, the substantial connection is also considered to exist if the service provider has a significant number of users in one or more Member States or if it targets its activities towards one or more Member States of the Union. Thereby, the Regulation provides a number of evaluation criteria by which to determine such a substantial connection. This may be, for instance, the use of the local language/local currency, the possibility of ordering goods or services, the availability of applications in the local app store, or advertising activities.[26] However, the mere fact of having an online presence accessible in the Union, such as a website or an email address, taken in isolation, cannot be considered sufficient to determine that a service provider is offering services in the Union within the meaning of the Regulation.[27]

### b) Issuing authority and issuing conditions (Articles 4, 5, and 6)

The question of who is authorised to issue a European Production Order or a European Preservation Order depends on the choice of instrument and the category of data requested. The reason for this differentiation can be explained with the different scope of the respective measure and the differing intensity and impact on fundamental rights of the various data categories.

*European Production Order*

A European Production Order may be issued by a judicial authority[28] – in the reading of the Regulation this is a judge, a court, an investigating judge, or a public prosecutor – if it concerns subscriber data and certain types of traffic data, namely data requested for the sole purpose of identifying the user, such as IP addresses and access numbers. In specific cases, the European Production Order may be also issued by any other competent authority in the issuing state acting as an investigating authority authorised under national law to order the gathering of evidence in criminal proceedings. In such event, however, the Order needs to be validated by a judicial authority, as set out above, who must examine the conformity of the Order with the conditions under the Regulation, and, if applicable, national law.

When the Order concerns the more intrusive categories of data – traffic data[29] and content data –, the issuing authority may be only a judge, a court, or an investigating judge but not a public prosecutor. Similarly, as above, the issuing authority may, in specific cases, be any other competent authority under national law, provided that the Order is duly validated by a judge, court, or investigating judge in the issuing Member State.

The Regulation departs from this mechanism in validly established emergency cases.[30] In the event of an emergency case, the issuing authority may, as an exception, issue a European Production Order in respect of subscriber data and data requested to identify a user without prior validation by a judicial authority if the validation could not be obtained on time and if the issuing authority could issue such an order in similar domestic cases without prior validation. In such a case, the issuing authority needs to obtain an *ex-post* validation without undue delay, at the latest within 48 hours. If the *ex-post* validation is not granted, the Order shall be withdrawn and the data obtained deleted or its use restricted.

The conditions for issuing a European Production Order differ according to the category of data: For subscriber data and user identification data,[31] a European Production Order may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least four months.

In respect of the more intrusive traffic and content data, a European Production Order can only be issued for criminal offences punishable in the issuing Member State by a custodial sentence of a maximum of at least three years. In addition, in respect of specific enumerated offences, a European Production Order may be also issued irrespective of the scale of the custodial sentence if the offences were committed by means of an information system. The list of enumerated offences includes fraud and counterfeiting of non-cash means of payment,[32] sexual abuse and exploitation of children,[33] attacks on IT systems,[34] and terrorist offences[35]. A European Production Order may also be issued for the execution of a custodial sentence or detention order of at least four months imposed for said enumerated criminal offences.

In addition to the more formal requirements on the information to be provided in the Order, there are also important limitations to the issuing of the European Production Order. These limitations concern situations in which the data is stored or processed by a service provider as a service to a public authority. In this case, the Order may only be issued if the public authority is located in the issuing Member State. Similar limitations apply to data stored or processed for professionals protected by professional privileges. The Regulation envisages a consultation procedure between the issuing authority and another Member State, in which the requested traffic or content data could be protected under immunities and privileges granted under the law of that other Member State, which applies to the service provider.

Irrespective of the category of data, the issuing authority needs to conduct a necessity and proportionality test and take into account the rights of the suspect or accused person. Lastly and importantly, the European Production Order may be only issued if a similar order could have been issued under the same conditions in a similar domestic case.

*European Preservation Order*

By contrast, in the case of the European Preservation Order, a differentiation depending on the data categories does not exist. Accordingly, the European Preservation Order may be ordered for all categories of data by a judicial authority – judge, court, investigating judge, or public prosecutor – or, in a specific case, by any other competent authority in the issuing Member State that acts as an investigating authority and is authorised under national law to order the gather-

ing of evidence in criminal proceedings, provided that the Order has been validated by a judicial authority. The special rule governing emergency cases applies here in the same way as it does for the European Production Order.

The European Preservation Order may be issued if the issuing authority considers the Order necessary and proportionate for the purpose of preventing the removal, deletion, or alteration of data in view of a subsequent request for production, not only via the European Production Order but also via mutual legal assistance or a European Investigation Order. The rights of the suspected or accused persons must be taken into account. The European Preservation Order may be issued in respect of all criminal offences, provided that it could have been ordered under the same conditions in a similar domestic case and for the execution of a custodial sentence or a detention order of at least four months.

The conditions for the issuing of a European Preservation Order envisage a mandatory set of information to be provided with the Order, similar to but less comprehensive than that for the European Production Order. The Regulation also provides for a limitation on data stored or processed for a public authority; however, there is no such limitation in respect of professionals protected either by a professional privilege or by other types of privileges. The latter aspect should, however, be duly considered during the obligatory necessity and proportionality check to be conducted by the issuing authority in the process of issuing the Order.[36]

### c) Addressees of the Orders and addressees' obligations (Articles 7, 10, and 11)

Addressees of the European Production and Preservation Orders are the designated establishments or legal representatives of the service providers.[37] In emergency cases,[38] the Orders may be directed to any other establishment or legal representative of the service provider, if the designated establishment or legal representative do not react or have not yet been designated.[39]

As regards the obligations, the European Production Order constitutes a binding decision of an issuing authority of a Member State obliging a service provider to produce electronic evidence within 10 days, or eight hours in emergency cases. Notification of the enforcing Member State pursuant to Art. 8 of the Regulation develops a suspensive effect on these obligations, save for emergency cases.[40] However, the strict deadlines imposed upon the service providers do not, in effect, change if the enforcing Member State does not raise any grounds for refusal. This means that service providers may need to be prepared to preserve and produce the requested data within the set 10-day period. If the service provider transmitted data to the issuing authority, while the enforcing Member State subsequently raised a valid ground for refusal, such data must be deleted or otherwise restricted, or, in the event that the enforcing authority has specified conditions, the issuing authority must comply with these conditions when using the data.[41]

The Regulation provides for a consultation mechanism, but no grounds for refusal, in the event that the service provider raises legal, formal, or factual impediments when complying with its obligations to execute the European Production Order. Accordingly, if the service provider raises concerns that the European Production Order could interfere with immunities and privileges, or with rules on freedom of the press or freedom of expression in the enforcing Member State, it shall inform both the issuing and the enforcing Member State. In such a case, the issuing authority may decide on its own motion or on request by the enforcing authority to withdraw, adapt, or maintain the Order. The enforcing authority may also decide to invoke a ground for refusal, provided it has such a right under Art. 8 of the Regulation. A similar consultation mechanism also applies in situations in which the service provider cannot comply with the European Production Order because the Order is incomplete, contains manifest errors or insufficient information, or because it is *de facto* impossible to execute it.

Generally, whenever the service provider for any other reason does not provide the requested information or cannot meet the deadline, it shall inform the issuing authority as well as the enforcing authority referred to in the Order to settle the matter expeditiously. In any case, the service provider has to preserve the data until it is produced, unless the service provider is informed that the preservation is no longer necessary.

Likewise, the European Preservation Order also constitutes a binding decision on a service provider, with the difference being the aim to preserve electronic evidence, with a view to a subsequent request for production via mutual legal assistance, a European Investigation Order, or a European Production Order. To this end, the service provider is obliged to preserve the requested data for a period of 60 days, after which the preservation shall cease. However, if the issuing authority confirms that a European Production Order has been already issued, the service provider needs to preserve the data as long as necessary in order to be able to produce it. In the event that a European Production Order has not yet been issued, the issuing authority may extend the initial 60-day period to preserve the data for an additional 30 days, with the aim of issuing the Order. As in the case of the European Pro-

duction Order, the Regulation envisages also a consultation mechanism in the event that the service provider raises legal, formal, or factual impediments to comply with its obligations to execute the European Preservation Order.

### d) Notification and grounds of refusal of the enforcing Member State (Articles 8 and 12)

A point fervently discussed during the negotiations concerned the extent of the involvement of competent authorities in the enforcing Member State and, in particular, whether the enforcing Member State should have any grounds to refuse the execution of the Orders. While the initial Commission proposal did not envisage any role for the enforcing Member State other than to facilitate the enforcement of the Orders, Art. 8 of the Regulation now stipulates situations in which the enforcing Member States must be notified and Art. 12 grants that Member State specific grounds to refuse the enforcement of a European Production Order.

Thus, whenever a European Production Order is issued for the production of traffic[42] or content data, the issuing authority needs to notify the competent authority of the enforcing Member State and transmit the European Production Order Certificate[43] at the same time it is transmitted to the service provider. The issuing authority also needs to include any additional information that enables the enforcing authority to assess the possibility of raising a ground for refusal. The notification of the enforcing Member State has a suspensive effect[44] on the obligation of the service provider, unless the matter concerns an emergency case, as defined in Art. 3(18).

The Regulation defines however an important exception from the notification requirement: there is no need to notify, if there are reasonable grounds at the time of issuing the Order that the offence was, is being, or is likely to be committed in the issuing Member State and that the person whose data is sought resides in that Member State (residence criterion).[45] Cases that do not affect the enforcing Member State should not lead to a notification. Similarly, the nationality of the person whose data is sought does not play a role.[46] The assessment of whether or not this exclusion is applicable rests solely with the issuing authority and, in this way, the issuing authority determines whether the competent authority in the enforcing Member State is granted the possibility to raise grounds of refusal of the European Production Order.

The grounds for refusal granted to the enforcing Member State are limited to reasons related to the principle of *ne bis in idem,* privileges and immunities, freedom of press and freedom of expression, and fundamental rights – whereby this latter reason is particularly subject to various limiting caveats.[47] In addition, Member States may invoke a refusal ground if the conduct for which the Order was issued does not constitute an offence under the law of the enforcing Member State (double criminality). The double criminality ground cannot, however, be invoked in relation to specific listed categories of offences[48] that are punishable with a custodial sentence or a detention order for a maximum period of at least three years in the issuing Member State. The enforcing authority is required to raise its grounds for refusal[49] within a period of ten days, or 96 hours (four days) in emergency cases, failing which it is deemed that the grounds for refusal have not been raised.[50] The ensuing effect of raising the grounds for refusal is that the service providers must halt the execution of the Order and refrain from transferring the data to the issuing authority, while the latter is requested to withdraw the Order. The Regulation also envisages a consultation mechanism between the enforcing and issuing authorities prior taking the decision on raising the grounds for refusal. This allows the competent authorities to find appropriate ways to overcome any potential grounds for refusal by adapting the Order or withdrawing it entirely.

### e) Enforcement and penalties procedure (Articles 15 and 16)

The Regulation establishes an enforcement procedure and a penalties regime in the event that the service provider fails to comply with the duty to execute a European Production or Preservation Order Certificate (hereinafter: "EPOC" and "EPOC-PR").[51] The same applies if the service provider fails to comply with the duty to set up state-of-the-art operational and technical measures to ensure confidentiality, secrecy, and integrity of the transmission of the documents and data produced or preserved, as envisaged in Art. 13(4). In so doing, the Regulation obliges the Member States to lay down the rules and measures for such pecuniary penalties and to notify the Commission thereof without delay.

The Regulation stipulates only that the penalties regime has to provide for effective, proportionate, and dissuasive pecuniary penalties; it generally leaves the possibility for sanctioning, including by means of criminal law, to national law. Still, the Regulation clarifies that the pecuniary penalty may amount to up to 2% of the total annual worldwide turnover of the service provider. Only if a service provider acts in good faith when complying with the requirements of the EPOC and EPOC-PR, it shall not be held liable for the prejudices to their users or third parties – without prejudice to the applicable data protection obligations.

In case of non-compliance with the duties under the Regulation, the issuing authority may request the competent authority in the enforcing Member State, i.e., the State in which the designated establishment has been established or in which the legal representative resides, to enforce the Order. To this end, the issuing authority needs to send to the enforcing authority the Order accompanied by the form in which the service provider outlines the reasons for the non-execution of the EPOC or EPOC-PR (Annex III to the Regulation) as well as any other relevant documents. Based on this information, the enforcing authority is obliged to recognise the Order as it is and take the necessary measures for its enforcement without undue delay, no later than five working days after receipt of the Order. To that end, the enforcing authority formally addresses the service provider and requests that it complies with the obligations by a set deadline. The enforcing authority also needs to inform the service provider about the penalties in case of non-compliance and about the possibility to oppose the execution for specific reasons,[52] as outlined in Art. 16(4) and Art. 16(5) of the Regulation.

In addition, the enforcing authority may itself deny the enforcement if it considers any of the grounds for denial stipulated in Art. 16(4) and Art. 16(5) to apply to the matter brought before it. These grounds for denial include those for formal and material reasons, such as incorrect issuing or validation of the Order, *de facto* impossibility to execute the Order, service that is out of scope of the Regulation, or a manifest breach of fundamental rights.

On the basis of the information available or additionally provided, the enforcing authority shall decide whether or not to enforce the Order or deny its recognition and notify the issuing authority and the service provider accordingly. In case of non-recognition, the Regulation envisages a consultation procedure with the issuing authority similar to the one for grounds for refusal. In case of enforcement, the enforcing authority is to obtain the data from the service provider and, in the event of non-compliance, impose pecuniary penalties in accordance with the penalties system provided under Art. 15. The penalty is subject to an effective judicial remedy and the service provider may take action against it.

### f) Review procedure in case of conflicting obligations (Article 17)

The issuing of a European Production Order must comply with the conditions laid out in the Regulation and, to the extent required, national law as well as with fundamental principles.[53] It may be the case, however, that the European Production Order is in conflict with the laws of a third state, which prevents the service provider receiving the Order from executing it. This is particularly the case when large service providers are involved that operate in several jurisdictions and that are bound not only by EU law but also by their domestic laws.

In such situation, Art. 17 envisages that the service provider informs the issuing and enforcing authority and provides a reasoned objection within a period of ten days, which includes details on the law of the third state applicable to the case as well as the nature of the conflicting obligation. The mere circumstance that similar provisions governing the issuing of a production order for the purpose of gathering electronic evidence do not exist in the third state or the fact that data is stored there do not suffice.

Upon provision of the reasoned objection, the issuing authority must review the Order it had submitted against the reasons provided in the reasoned objection. If the issuing authority intends to uphold the Order, it needs to refer the matter to the competent court in its Member State. The execution of the Order is suspended pending the review procedure.

In the judicial proceedings, the competent court has to make an assessment as to whether the law of the third country applies in the case at hand at all and, if so, whether it prohibits disclosure of the data concerned. Should the court conclude that the law of the third state constitutes such prohibition, the court needs to strike a balance between the conflicting interests based on criteria set in the Regulation. These criteria concern the underlying interests behind the prohibition, including the protection of fundamental rights and national security of the third state, the degree of connection with the respective jurisdictions, the degree of connection of the service provider and the third country, the interest in pursuing the investigations, and the consequences for the addressee and/or service provider, if it/they were to comply with the Regulation in violation of the laws of the third state.

To facilitate the assessment to be carried out by the court, the Regulation envisages that the court may seek information from the third state, without prejudice to the investigations. The court is even obliged to contact the third country authorities in the event the matter concerns fundamental rights or fundamental interests of state security of the third state.

Upon reaching its decision, the court shall inform the issuing authority, the service provider, and the enforcement authority of its decision. Although the Regulation does not envisage any obligation to inform the authorities of the third state, it may be assumed that information about the outcome of the proceedings will also be provided to those au-

thorities, at least if there was relevant contact in the course of the review proceedings.

Needless to say, this matter and this procedure, whereby the court takes into account the law and interests of a third state, touch upon a complex and politically sensitive area. Given that many large service providers are located outside the Union, most notably in the USA, the conflicting obligations described above are likely to occur frequently. In order to avoid clashes with foreign jurisdictions, the EU should seek to establish greater certainty in respect of affected foreign jurisdictions as a matter of urgency (see to this effect below under V.1).

### g) Rights of the person whose data is sought (Articles 13 and 18)

The Regulation already states in Art. 1(3) that fundamental rights and legal principles enshrined in the Charter and in Art. 6 of the Treaty on European Union will be fully safeguarded. Moreover, the entire set of EU directives for procedural rights in criminal proceedings[54] will also apply.

The person whose data is sought will, however, generally not be in a position to find out whether his/her data was subject to the measures under the Regulation. Art. 13(1) hence requires that the issuing authority inform that person without undue delay. When informing the person, the issuing authority has to include information about available remedies pursuant to Art. 18 of the Regulation. The issuing authority may, however, delay, restrict or omit informing the person whose data is sought to the extent and under the conditions of Directive 2016/680[55], primarily in order not to prejudice the criminal investigations. In such case, the issuing authority needs to indicate the reasons in the case file and provide a short justification in the Certificate.[56]

In this context, Art. 18 provides for effective remedies against measures imposed under the Regulation. This provision enables the person whose data was sought to challenge the legality of a measure, including its necessity and proportionality, before the competent court in the issuing Member State, no matter if the person concerned resides elsewhere. This right is without prejudice to the guarantees of fundamental rights also in the enforcing State.[57] If that person is a suspect or accused, he/she may make use of all the rights granted to it during the criminal proceedings for which the data was ordered.

Additional remedies may also follow from the General Data Protection Regulation[58] and Directive 2016/680, as well as legal remedies available under national law, whereby the same time limits and conditions for seeking a remedy in similar domestic cases apply. This aims to guarantee an effective exercise of the remedies for the persons concerned.[59]

Art. 18 makes an explicit reference only to the European Production Order, and it is unclear whether and if so to which extent effective remedies against a European Preservation Order are available.

Although the Regulation puts an explicit obligation on the issuing Member State and any other Member State, to which electronic evidence was transmitted, to ensure that the rights of defence and fairness of the proceedings are respected when assessing the evidence obtained, the approach taken on the availability of effective remedies is therefore somehow unsatisfactory.

### h) Standardised and IT-driven procedure – certificates and decentralised IT system (Article 9, Chapter V and Annexes)

The Regulation also formalises the procedure by establishing a decentralised IT system and by annexing standard forms to be used when applying this new mechanism.

The decentralised IT system aims to ensure a swift, direct, and secure cross-border electronic exchange of case-related forms, data, and information. It will be comprised of the IT systems of Member States and of the Union's agencies and bodies in addition to interoperable access points through which they are connected. The designated establishments or legal representatives designated by the service providers will be able to access the national IT systems forming part of the decentralised IT system. Art. 22 of the Regulation entrusts the Commission with the creation, maintenance, and development of a reference implementation software, which Member States may apply instead of a national IT system. This measure, too, strives towards the greatest possible coherence in the practical application of the e-evidence rules.

Although communication and exchange, as a rule, are to take place via the decentralised IT system, there might be cases in which this is not possible, e.g. due to the disruption of the system, the nature of the transmitted material, technical limitations, legal constraints related to the admissibility of evidence, or exceptional circumstances.[60] In such a case, the Regulation states that the transmission shall be carried out via the most appropriate alternative means, taking into account the need for swiftness, security, and reliability of the exchange of information. Any transmission by alterna-

tive means shall be recorded in the decentralised IT system without undue delay.

The use of electronic communication means for the transmission of documents is flanked by Arts. 20 and 21, which state that such documents should be granted legal effect and be considered admissible in the context of cross-border judicial procedures under the Regulation. A qualified electronic seal or qualified electronic signature, as defined in Regulation (EU) No 910/2014,[61] is to be used.

In addition, the desired swift, direct, and secure cross-border communication and exchange is facilitated by providing a set of standardised documents, annexed to the Regulation, including the EPOC and the EPOC-PR, through which the Preservation and the Production Orders have to be transmitted. The certificates contain information relevant for the execution of the Orders, such as details on the issuing authority, the user, the requested data category and time range, the applicable law, reasons given in case of emergency, the grounds for the necessity and proportionality of the measure, and, in the case of the EPOC, the summary description of the case.[62] The certificates will be available in all official languages of the Union, and Member States may decide, at any time, that they will accept translations of EPOCs and EPOC-PRs, not only in their own official language but in one or more official language(s).[63]

#### i) Costs (Articles 14 and 23)

In view of the central role given to the service providers when gathering evidence for the purpose of criminal proceedings, the Regulation envisages in Art. 14 a reimbursement scheme, based on which the service providers may claim reimbursement of their costs from the issuing Member State. Reimbursement is only granted, however, if this possibility is provided for in the national law of the issuing Member State for domestic orders in similar cases. Hence, whether and, if so, to what extent such reimbursement will be granted in practice will depend on the situation in the issuing Member State. The national practice often ranges from full reimbursement to full bearing of the costs.[64]

Another type of cost concerns costs related to the decentralised IT system. The decentralised IT system is essential for the written communication and data exchange between the competent authorities and the service providers as well as among the competent authorities themselves. Ensuring confidentiality, secrecy, and integrity of the transmissions of the documents and the data produced or preserved requires, in particular, that the service providers install state-of-the-art operational and technical measures, which, if not in place, may be sanctioned under Art. 15 of the Regulation. With regard to costs, Art. 23 envisages that each Member State, Union agency or body, and each service provider bears all costs related to the use and maintenance of or the interaction with the decentralised IT system, as the case may be.

### 2. Directive on the designation of establishments and appointment of legal representatives

While the Regulation regulates the rules under which the authority of a Member State may order a service provider offering services in the Union to produce or preserve electronic evidence for the purpose of criminal proceedings, the accompanying Directive lays down the rules and obligations ensuring that the orders and decisions issued under the Regulation reach the right addressees: the private service providers.[65] The aim of this legal act is to guarantee a coherent approach to imposing obligations on service providers – and Member States – in the context of gathering electronic evidence in criminal proceedings. The approach seeks to overcome the problems that previously resulted from the existence of different national rules and obligations and the fact that many service providers, though operating in the Union, are located outside the bloc.

By setting out the rules on the designation of establishments and the appointment of the service providers' legal representatives, the Directive establishes a clear channel of communication, and thus the necessary legal certainty, not only for the service providers, who were often uncertain whether they were obliged or allowed to follow up on a request in the past, but also for the competent national authorities across the Union, who may now quickly and efficiently direct their requests to the correct addressee.

This central element of the Directive – the designation of establishments and appointment of legal representatives by service providers – is flanked by the obligation for the Member States to set up a penalties regime to deal with any violation of the obligations under the Directive. They are also required to designate central authorities mandated to ensure a consistent and proportionate application of the Directive.

Although the Directive clearly pursues the purpose of facilitating the work of national authorities in gathering electronic evidence in criminal proceedings, it is based on Arts. 53 and 62 TFEU, which guarantee the freedom to provide services. This is explained somewhat briefly in the Explanatory Memorandum of the Commission Proposal where it is stated that the obligations following from the Directive

would help eliminate obstacles to the freedom to provide services.[66] This choice of legal basis was subject to criticism during the negotiations, but, as it was the case with the Regulation, was not changed by the legislator.

### a) The designation of designated establishments and legal representatives by the service providers (Articles 3 and 4)

The Directive states that Member States need to ensure that service providers offering services in the Union designate at least one addressee for the receipt of, compliance with, and enforcement of decisions and orders issued by the competent authorities of Member States for the purpose of gathering evidence in criminal proceedings. To this end, the Directive targets the same service providers as those covered under the Regulation.[67]

Service providers that are established in the Union[68] and provide services in more than just one Member State[69] are requested to designate one or more designated establishments to be responsible for carrying out the functions described in the Directive. Service providers that are not established but offer their services in the Union (this applies to many large companies located in the USA) are required to appoint one or more legal representatives to be responsible for carrying out the functions described in the Directive. Thereby, the term "offer services in the Union" has the same meaning as that provided under the Regulation.[70] In the event that a service provider is established in a Member State that does not take part in the e-evidence package the service provider needs to appoint a legal representative in a Member State that does take part in this instruments.

The service providers are, in principle, free to choose how many designated establishments or, as applicable, legal representatives they designate or appoint and in which Member State(s). Member States cannot restrict this free choice.[71] For the purpose of operationality, however, the Directive states that the designated establishment should be established in a Member State in which the service provider provides its services or is established, and it should designate a designated establishment in one of the Member States taking part in a legal instrument referred to in the Directive (see below).[72] The same applies to the legal representative.[73] To ensure clarity, service providers must indicate the precise territorial scope of the designation, in the event that they designate several designated establishments or appoint several legal representatives, respectively.[74]

The Directive also allows for a designated establishment or legal representative to be shared by several service providers, unless this would impinge on data protection safeguards. This possibility for sharing may be particularly beneficial to small-sized and medium-sized enterprises.[75]

Although established by the Directive as part of the e-evidence package, the role of designated establishments and legal representatives is, pursuant to Art. 1(2), not confined to decisions and orders under the Regulation alone but may also apply in the context of the European Investigation Order[76] and the EU Convention on Mutual Legal Assistance.[77] Moreover, this concept may equally apply to decisions and orders for the purpose of gathering electronic evidence on the basis of national law.[78] However, this means that the procedures set out in the instruments mentioned come to application. It is then to ask whether these instruments permit the direct serving of orders in cross-border situations to the designated establishment or legal representative or whether they demand cooperation between competent judicial authorities.[79]

Accordingly, the service providers must take all measures to ensure that the designees/appointees are equipped with the necessary powers and resources to comply with the decisions and orders received from the authorities of any Member State participating in the instruments mentioned above. Member States are under a duty to verify whether this is and will remain the case (see also central authority below).

In terms of procedure, each service provider must notify the central authority in writing (see below) within a period of six months from the transposition deadline of the Directive or from the moment it starts offering services in the Union[80] about the Member State in which it is established or offers its services and where its designated establishment is established or where its legal representative resides, respectively. The notification should also provide information about the languages to be used[81] and the precise territorial scope of its designation.[82]

### b) Penalties regime (Article 5)

Art. 5 of the Directive envisages a separate penalties regime in case there is a violation of the obligations imposed upon the service providers under the Directive. The Directive thereby clarifies that non-compliance cannot be justified on the grounds of, *e.g.,* inefficient internal procedures or lack of resources, insufficient powers, or the failure to notify a designated establishment or a legal representative. In case of non-compliance, the designated establishment or the legal representative and the service provider itself may be held jointly and severally liable, *i.e.,* each of them – the designated estab-

lishment or the legal representative and the service provider – may be sanctioned for non-compliance by any of them.[83]

The penalties to be imposed shall be effective, proportionate, and dissuasive. When determining the appropriate penalty, all relevant circumstances should be considered: the financial capacity of the service provider; the nature, gravity, and duration of the breach; whether it was committed intentionally or through negligence; and whether the service provider has been held responsible for similar previous breaches. Under no circumstances, however, should the sanctions envisage a permanent or temporary ban of the provision of services,[84] as it would run counter the very purpose of the Directive, the aim of which is to remove obstacles to the free provision of services in the Single Market.

Legal action following civil or administrative proceedings, including proceedings that can lead to sanctions, may, in principle, be applied in parallel to any sanctions under the Directive. In this context, the Directive also envisages a number of notification requirements for the Member States. Upon transposition of the Directive, Member States are obliged to notify the Commission of their rules and of measures enacted with regard to the sanctions regime; they must also provide updates should the rules be amended in the future. In addition, Member States have to inform the Commission annually about cases of non-compliance by service providers, the relevant enforcement action taken against them, and the sanctions imposed. These notification requirements should ensure the necessary transparency but also demonstrate the effectiveness of the measures.

#### c) Central authority (Article 6)

Member States are required to designate one or more central authorities to ensure a consistent application of the Directive and to ensure a seamless cooperation amongst the central authorities in other Member States, in particular by exchanging information and providing mutual assistance. This relates, in particular, to the enforcement actions as well as verifications of whether the designated establishments or legal representatives residing on their territory received from the service providers the necessary powers and resources. In this way it will be also apparent, whether the designated establishments or legal representatives cooperate with the competent authorities in accordance with the applicable legal framework.

To this end, the central authorities themselves are required to be equipped with sufficient powers to carry out the tasks entrusted to them, including coordination powers for enforcement actions between competent authorities in different Member States. For the coordination of an enforcement action, the central authorities may also involve the Commission if this could be relevant.[85] An additional aim of this coordination mechanism is to avoid positive or negative conflicts of competence amongst competent authorities in the Member States.

Furthermore, this new mechanism will also serve important transparency functions. The designation of the central authorities will make it easier for the service providers to provide notification about the designation and the contact details of their designated establishment or legal representative to the proper place in the Member State where their designated establishment is established or legal representative resides.

Accordingly, once Member States inform the Commission of their designated central authority or central authorities, the Commission will distribute a list of designated central authorities to all the Member States and make it also publicly available.

### IV. Implications for Stakeholders

With the adoption of the e-evidence package, the time period for implementation and adaptation has started. Ensuring that the full e-evidence framework is properly and accurately implemented in the European and national legal orders requires the necessary time and effort on the part of all stakeholders involved. As shown in the previous sections, the complex nature of the adopted rules and procedures call for a careful analysis of the rights and obligations of all actors affected as well as of the reasonable expectations they may have from each other.

One of the main initial points of criticism regarding this initiative concerned the protection of fundamental rights, particularly in light of the proposed mechanism of direct cooperation between private entities and public authorities for the purpose of law enforcement activities.[86] While the role of service providers – that hold an unprecedented strong position in handling and keeping vast amount of information – in the European legal order has increased significantly over the past several years,[87] the area of criminal justice was not familiar yet with a direct role of private entities in the enforcement activities of national authorities across the Union. Service providers will in this way have to play multiple and even contradicting roles: serving as the extended arm of public law enforcement authorities, protecting the personal data of their customers, and ensuring their own legitimate business interests. It is not far-fetched to imagine that clients might

wonder whether the service provider is sharing their personal data with law enforcement authorities and how they can find this out. The diverging interests might put the service providers in a difficult situation, and it remains to be seen how service providers will cope with this new role they have been given by the Union legislator with the e-evidence package and how they will strike a balance between the diverging interests. A procedure that remains largely confidential between the national authorities and the service provider, and hence undisclosed to the public, demands that greater attention be given to transparency and effective judicial review.

Whether this will be guaranteed in a satisfying manner remains to be seen. Just to give an obvious example: While the issuing authority should inform the person whose data is being sought about the data production without undue delay, the same issuing authority may decide, in accordance with national law, to delay, restrict, or even refrain from informing the person to the extent that/as long as the conditions of Directive 2016/680[88] are met. In practice, this means that the applicable rules vary per Member State and that the person whose data is being sought will not automatically know whether his/her data has been shared with law enforcement authorities, hence not be able to go against it. The person may not even find out that his/her data was sought in the first place if national law allows for omitting to inform the data subject for as long as "such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned". A mandatory (*ex post*) notification is not envisaged in the e-evidence package. If the person whose data is sought does become aware of the circumstance that his/her data was shared with national law enforcement and judicial authorities, the right to effective remedies against the European Production Order exist, including possible additional legal remedies in accordance with national law. For this specific situation, the rules stipulate that information should be provided in "due time" about the possibilities to seek remedies under national law and to ensure that they can be exercised effectively.

Although the involvement of judicial authorities in the enforcing Member State has increased with the adopted rules, particularly as regards the most sensitive data categories for which electronic evidence could be requested, the necessary judicial control might quickly fall short of the needed effectiveness. Situations involving several Member States could soon overburden the judicial control mechanism envisaged under the Regulation, e.g., when data is requested by Member State A, from a service provider located in Member State B, with the person residing in (but not being a national of) Member State C, and providing professional services in Member State D. At the time of the request, it may neither be known to the authorities in Member State A (issuing Member State), nor the ones in Member State B (enforcing Member State) that the person whose data is being requested is carrying out journalistic activities in Member State D. In this scenario, Member State C (place of residence) and Member State D (place of professional activity) would not receive any notification of the request sent to Member State B by Member State A. This raises the question of an effective legal remedy, as the question in which Member State(s) the person concerned should or could seek legal remedies may not always be straightforward. Concerns about the final package have indeed been raised as regards media freedom and the possible misuse of confidential data belonging to journalists.[89] Similar concerns are also valid for persons subject to professional secrecy, such as defence lawyers or medical professionals.

From a law enforcement perspective, the new rules definitely provide a speedier framework for requesting data for law enforcement purposes compared to traditional mutual legal assistance instruments or even the European Investigation Order. Practice, however, will show whether service providers will actually be able to produce certain sets of data under the conditions imposed by the EU rules, particularly when there is no generalised obligation to retain data[90] and when orders to produce data only arrive at service providers after the commission of an offence and at the start of a criminal investigation, as required under the Regulation. By then, the data may have already been erased or can no longer be produced by the service provider.

Notwithstanding the foregoing, service providers will be required to make the necessary adaptations to their organisational structures – particularly by ensuring the necessary resources – at the risk of financial sanctions. Apart from that, they will be required to respond to requests for data on the basis of a mandatory and decentralised IT platform; the Commission will need to prepare implementing acts on this within two years after adoption of the Regulation.[91] Service providers should also be mindful of the possibility to claim reimbursement from the issuing State, in accordance with the national law of that State, of their costs for responding to a European Production Order or to a European Preservation Order if that possibility is provided for in the national law of the issuing State for domestic orders in similar situations (see above III.1 i)). As rules can vary, Member States are required to communicate to the Commission their national rules, which must also be made public. In view of the broad scope of EU rules and the high number of companies covered – telecommunication providers, cloud services, and over-the-top services –, these rules are expected to have a significant impact on the operationality of service providers.

## V. International Dimension

The borderless and open character of modern technology has the effect that cybercrime is becoming increasingly transnational, involving offenders and victims located in multiple jurisdictions. To adapt to these circumstances, it is important that cross-border access to electronic evidence by competent authorities follows a consistent set of rules which can ideally stand the test of time. Various efforts to improve access to electronic evidence for the purpose of investigating and prosecuting cross-border cases have already been undertaken, and recent developments show a continuation of these efforts at the national, European, and international levels. Based on the principle of mutual trust, the enacted e-evidence package is intended to set the standard in gathering electronic evidence for the purpose of criminal proceedings in the European Union. It would be in the interest of the EU to strive for high standards, including standards on data protection, at the international level as well. This section provides a brief overview of the existing international instruments that are relevant for the gathering of evidence in criminal proceedings. As will be seen, they also have an impact on the e-evidence package.

### 1. An EU-US E-evidence agreement

Finding a common approach between the EU and the USA that allows for cross-border access to data held by service providers in the EU or the USA has been an evergreen-priority on the justice and home affairs agenda. The United States of America are one of the main recipients, if not the main one, of mutual legal assistance (MLA) requests from EU Member States for access to electronic evidence, as the largest service providers are headquartered there. Given that the largest service providers are based in the USA and that the key instrument, namely mutual legal assistance between both continents, has its limits (notably its slowness),[92] this does not come out of blue. An EU-US e-evidence agreement could indeed help overcome current divergent approaches, which often rely on voluntary cooperation mechanisms between judicial authorities and service providers. Such an agreement could set common standards that also address conflicts of laws. Direct cooperation with service providers in the USA would be a significant improvement over the time-consuming classical mutual legal assistance process. Under the U.S. Stored Communications Act of 1986,[93] however, direct cooperation is limited to non-content data and the service providers are free to cooperate, while a disclosure of content data is prohibited. The United States CLOUD Act (Clarifying Lawful Overseas Use of Data), adopted on 23 March 2018, amends the Stored Communications Act of 1986 such that US service providers are obliged to comply with US orders to disclose content data and non-content data, regardless of where such data is stored, i.e., no matter whether the data is stored on servers located in the EU or not. The CLOUD Act allows the conclusion of executive agreements between the USA and foreign governments, on the basis of which US service providers would be able to deliver content data directly to the foreign governments. The scope of data covered by the CLOUD Act is stored data and the interception of wire or electronic communication with respect to serious crimes. The executive agreements are subject to a number of conditions, including that the domestic law of the third country and its implementation "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection".[94] So far, the USA has concluded executive agreements under the CLOUD Act with the UK[95] and Australia[96] and has entered into negotiations with Canada.[97] The executive agreements concluded, however, all contain an important restriction prohibiting the transfer of data concerning US citizens and persons located in the USA.

The Council Decision authorising the opening of negotiations for an EU and US agreement on cross-border access to electronic evidence, together with its negotiating directives,[98] was adopted swiftly after being proposed by the Commission in February 2019. While the Council largely followed the Commission's approach, it is interesting to note that, compared to the proposal, the Council introduced two additional procedural rights safeguards to be reviewed in conjunction with the scope of the future agreement: (1) safeguards to ensure that data requested may be refused if the execution of the request is likely to be used in criminal proceedings that could lead to life imprisonment without the possibility of review and prospect of release; (2) specific safeguards for data protected by privileges and immunities and data whose disclosure would be contrary to the essential interests of a Member State.[99]

After the adoption of the EU's negotiation mandate in June 2019, negotiations were put on hold for a number of years. This was due to the fact that the negotiating directives set out not only that compatibility between the EU-US agreement and the EU rules of the e-evidence package be ensured but also that these rules serve as the baseline for the Union's negotiating position. This is why an agreement on the e-evidence package had to be reached first, before it was possible to enter into in-depth negotiations on the EU-US agreement. The negotiations resumed in March 2023[100] and are currently ongoing.

Time has not stood still, however, since the negotiations between the EU and US were halted in 2019. There have

been a number of recent developments, including the fact that an agreement has been found on the Second Additional Protocol to the Budapest Convention (below 2.). The negotiating directives reflect in this respect that the future EU-US agreement should take precedence over the Budapest Convention as well as any agreement reached on the negotiations of the Second Additional Protocol, in so far as the provisions of the latter agreement cover issues dealt with by the EU-US agreement.[101] It is of relevance that the USA signed both the Budapest Convention and the Second Additional Protocol. Also noteworthy are the interconnection with the EU's data protection legislation and jurisprudence, including the General Data Protection Regulation (GDPR), and the recently adopted adequacy decision under the EU-U.S. Data Privacy Framework.[102] The same applies to the EU's approach towards digital sovereignty and cybersecurity.[103]

The conclusion of the executive agreement with the USA is essential for a seamless functioning of the e-evidence package. The agreement particularly has to clarify the binding nature of orders on service providers and also define the obligations for judicial authorities. It is hence indispensable that the negotiations with the USA on the executive agreement come to a timely conclusion, before the coming into application of the e-evidence package.

### 2. The Council of Europe Convention on Cybercrime ("Budapest Convention")

Following the adoption of the Budapest Convention in 2001, and its entry into force in 2004, 68 States have become official parties to the treaty to date.[104] According to its Explanatory Memorandum, the Convention aims to (1) harmonise the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime, (2) provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form, and (3) set up a fast and effective regime of international cooperation.[105] Despite its relative 'old' age, the Convention has not lost its relevance in modern practice, thanks to its technology-neutral language and high number of participating States.

Since its adoption 22 years ago, the Convention has been updated twice: The First Additional Protocol in 2002 extended the scope of the "mother Convention" by criminalising acts of a racist and xenophobic nature committed through computer networks. The Second Additional Protocol was adopted by the Committee of Ministers on 17 November 2021.

The Second Additional Protocol intends to step up the fight against cybercrime by strengthening the possibilities for judicial authorities to collect electronic evidence of a criminal offence for the purpose of specific criminal investigations or proceedings by means of additional tools, e.g., the possibility for two or more parties to establish a joint investigation team and the taking of testimonies and statements of witnesses or experts by video conference. In addition, the Second Additional Protocol provides rules on cooperation in emergency situations requiring an expedited response as well as rules on direct cooperation between competent authorities and service providers and entities in possession or control of pertinent information, including domain name registration information and subscriber data.

While the Convention applies only to the States that have ratified it and does not allow the EU to accede to it, the EU takes part in meetings of the Convention Committee as an observer and is committed to the Convention's promotion. The EU has played an essential role in ensuring that the Second Additional Protocol is coherent and consistent with Union law. Following up on the European Council Conclusions of October 2018,[106] the Commission adopted in February 2019 a Recommendation for a Council Decision with negotiating directives authorising the participation of the Commission, on behalf of the EU, in the negotiations on the Second Additional Protocol.[107] At the JHA Council in June 2019, the Council gave its green light to the Commission to negotiate this instrument.[108] Compared to the Commission proposal for the negotiating directives, it should be noted that the Council added Art. 16 and Art. 82(1) TFEU as legal bases as well as specific rules on the procedure for negotiations.[109] The adoption of the Council Decision on 5 April 2022 ultimately authorised EU Member States to sign the Protocol.[110] The Protocol was opened for signature in May 2022 and has been signed by 37 States to date.[111] The Council Decision to authorise Member States to ratify the Protocol was adopted on in February 2023 in accordance with the procedure laid down in Art. 218(6) TFEU. The European Parliament gave its consent in January 2023, after it voted against referring the Protocol to the CJEU for an Opinion in November 2022.

The Second Additional Protocol will complement the EU rules on the e-evidence package. It has the benefit that, once fully ratified, it will apply globally to all 68 signatory countries of the Budapest Convention.

### 3. The United Nations Cybercrime Convention

The idea behind and push for having a UN Convention on Cooperation in Combating Cybercrime in place came from

the Russian Federation in 2017.[112] Before the decision was taken to cease the Russian Federation's membership on the Council of Europe in response to its war against Ukraine,[113] the Russian Federation was the only member not party to the Budapest Convention; the Russian Federation held the view that the Convention encroaches upon its security and sovereignty.[114] In this light and coinciding in 2017 with the timing for launching negotiations on the Second Additional Protocol to the Budapest Convention, Russia's proposal for an international convention on cybercrime can only be regarded as an attempt to put in place a competing instrument. With 88 votes in favour to 58 against and 34 abstentions, the draft resolution of the Russian Federation was, nonetheless, adopted on 18 November 2019.[115]

Just one month later, the UN General Assembly adopted a resolution to establish an open-ended *ad hoc* intergovernmental committee of experts/representative of all regions to elaborate a comprehensive international convention on countering the use of information and communication technologies for criminal purposes (hereinafter: the UN Cybercrime Convention).[116] The agreement that a draft convention should be provided and the work schedule of the *ad hoc* committee were both endorsed by the General Assembly in May 2021.[117] If adopted, the Cybercrime Convention would be the first instrument at the UN level to combat cybercrime and would facilitate international judicial cooperation in criminal matters with third countries that are not party to the Budapest Convention and its Protocols. The proposed structure includes chapters on general provisions, criminal offences, procedural measures and law enforcement, international cooperation, technical assistance, preventive measures, mechanisms of implementation, and final provisions.[118]

With all EU Member States voting against the Resolution adopted by the UN General Assembly in 2019, the coordination of a uniform European position in the negotiations of the UN Cybercrime Convention is of crucial importance. In March 2022, the Commission issued a recommendation for a Council Decision with negotiating directives,[119] based on Art. 218(3) TFEU, allowing the Commission to negotiate the Convention on behalf of the EU. Two months later, the Council adopted its Decision,[120] adding Arts. 82(1) and (2) as well as Art. 83(1) TFEU as legal bases, taking into consideration that the new instrument may also affect EU rules on judicial cooperation in criminal matters. The Decision specifies in this regard that the Commission is to conduct negotiations on behalf of the EU for matters falling within its competence, in accordance with the Treaties and in respect of which the Union has adopted rules.[121] The guiding principles underpinning the EU's mandate refer most notably to establishing consistency with existing legislation, to guaranteeing a strong protection of human rights standards and fundamental freedoms, and to ensuring that definitions and procedures are sufficiently clear and specific.

With five negotiation sessions held so far, progress has already been made on the text of the draft Convention. The consolidated negotiating documents presented prior to the fourth and fifth sessions as well as the draft text of the Convention presented ahead of the sixth session[122] show how the Convention is taking shape, taking into account different proposals and statements, including those of the EU and its Member States.[123] The most recent consolidated negotiating document focused, amongst other things, on international cooperation and was published on the last day of the fifth session of the Ad Hoc Committee on 21 April 2023.[124] This document shows the sensitivities and complexities of the negotiations, including attention to the protection of personal data, extradition, and mutual legal assistance procedures. It also shows the committed approach of the EU and its Member States towards safeguarding fundamental rights and values. The plan is for the text of the future Convention to be finalised during a concluding session at the beginning of 2024 with a view for its adoption in September 2024. It remains to be seen whether the final text of the UN Convention will be consistent with and provide any added value to the existing international and EU legislative instruments, such as the Budapest Convention and its protocols.

## VI. Conclusion

The adoption of the EU e-evidence rules is an important step forward towards facilitating effective cross-border cooperation in criminal matters, which, given the borderless dimension of criminal activity, is sure to become even more pressing over the next several years and decades. With the costs stemming from the (mis-)use of digital technologies for the purpose of committing crimes alone are expected to rise from 8.4 trillion US dollars in 2022 to 10.5 trillion US dollars by 2025,[125] it is clear that the fight against this growing phenomenon should be given a high priority at all levels. The newly adopted rules require all stakeholders – from judicial and law enforcement authorities to service providers and defence lawyers – to undertake all necessary efforts to ensure their timely and accurate implementation as well as their correct application in practice. The mechanism established under the e-evidence rules relies fundamentally on the principle of mutual trust among the EU Member States and a presumption of their compliance with Union law, the rule of law, and fundamental rights and values. It is of particular significance that five Member States issued statements upon adoption in which they express concerns regarding the pro-

tection of fundamental rights and the application of effective judicial review under the e-evidence package.[126] Hence, the application of the e-evidence package will require constant scrutiny, monitoring, and cooperation between all actors involved. Guaranteeing the necessary transparency and effective judicial review are key elements of this initiative. The practical application of these rules as well as ensuring coherence and consistency with initiatives at the international level – in particular the envisaged executive agreement between the EU and the USA – are, no doubt, essential components to effectively fight crimes in the European Area of Freedom, Security and Justice – today and in the future.

**Adam Juszczak**
DG Taxation and Customs Union
European Commission

**Elisa Sason**
Policy Officer, Security Union,
Secretariat-General
European Commission

* The views expressed in this article are solely those of the authors and are not an expression of the views of their employer or the institution they are affiliated with.

1 COM(2020) 605 final on the EU Security Union Strategy; COM(2021) 170 final on the EU Strategy to tackle Organised Crime; JOIN(2020) 18 final on the EU's Cybersecurity Strategy for the Digital Decade; COM(2020) 795 final on A Counter-Terrorism Agenda for the EU.

2 June 2016 Conclusions on improving criminal justice in cyberspace: <https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf>. All references to hyperlinks were last accessed on 16 October 2023.

3 European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)) – P8_TA(2017)0366.

4 Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final and proposal for a Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final.

5 SWD(2018) 118 final on the Impact Assessment accompanying the e-evidence package.

6 See, for example, the statement of civil society organisations and bar associations of 4 March 2022: <https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2022/Coalition's%20remarks%20on%20EP%20package%20deal.pdf>.

7 <https://www.euractiv.com/section/digital/news/council-makes-half-hearted-agreement-on-e-evidence/>.

8 Council General Approach text of 12 December 2018: <https://data.consilium.europa.eu/doc/document/ST-15292-2018-INIT/en/pdf>.

9 European Parliament, Report – A9-0256/2020 of 11 December 2020: REPORT on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.

10 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *O.J.* L 191, 28.7.2023, 118; Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *O.J.* L 191, 28.7.2023, 181.

11 Art. 34(2) of the Regulation.

12 Art. 7(1) of the Directive.

13 In accordance with Protocol No 22 on the position of Denmark annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

14 Cf. Recital 12 of the Regulation.

15 For the references of both acts in the Official Journal, see *op. cit.* (n. 10).

16 Cf. *e.g.*, M. Böse, An assessment of the Commission's proposals on electronic evidence, <http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf>; P. Topalnakos, "Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings", in this issue.

17 Art. 3(1) and (2) of the Regulation.

18 Art. 3(8) of the Regulation.

19 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *O.J.* L 201, 31.7.2002, 37.

20 Most notably the Convention on Cybercrime of the Council of Europe (CETS No. 185) – "Budapest Convention".

21 As defined in Art. 2(4) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, *O.J.* L 321, 17.12.2018, 36.

22 Such as "information society service providers" within the meaning of Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (*O.J.* L 241, 17.9.2015, p. 1).

23 Cf. Recital 27 of the Regulation.

24 Cf. Recital 28 of the Regulation.

25 Art. 3(4) of the Regulation.

26 Cf. Recital 30 of the Regulation.

27 Recitals 29 and 30 of the Regulation. The same considerations should apply to determine whether a service provider offers services in a Member State.

28 It is of note that, according to Art. 1(2) of the Regulation, the suspect or accused person or his lawyer may, under the defence rights afforded to him, request the issuing authority to issue a European Production Order or a European Preservation Order.

29 Except the data requested for the sole purpose of identifying the user as defined in Art. 3(10).
30 For the definition of the term "emergency cases", see Art. 3(18).
31 As defined in Art. 3(10) of the Regulation.
32 Directive (EU) 2019/713 of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, *O.J.* L 123, 10.5.2019, 18.
33 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA, *O.J.* L 335, 17.12.2011, 1.
34 Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *O.J.* L 218, 14.8.2013, 8.
35 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, *O.J.* L 88, 31.3.2017, 6.
36 Cf. to this end also Art. 11(4) of the Regulation.
37 For details, see below III.2.
38 As defined in Art. 3(18) of the Regulation.
39 Note: For reasons of clarity and simplicity, explanations in this section III.1 uses the term service provider and not addressee unless it is necessary to distinguish between the two terms. Further details on the designation are provided in section III.2 below.
40 Cf. Art. 8(4) of the Regulation.
41 Cf. Art. 10(4) of the Regulation.
42 Except for data requested for the sole purpose of identifying the user, as defined in Art. 3(10).
43 See below III.1 h).
44 Art. 8(4) of the Regulation.
45 Art. 8(2) and Recital 53 of the Regulation.
46 Cf., however, Art. 17(6)(b)(i) in relation to conflicts with the law of a third country, where the nationality is relevant. The language spoken might, however, play a role for the purpose of the rights of defence.
47 Art. 12(1)(b) refers to "exceptional situations", "substantial grounds", "specific and objective evidence", "particular circumstances of the case", requiring a "manifest breach". Evidently, the aim is to apply this refusal ground particularly narrowly.
48 Enlisted in Annex IV of the Regulation.
49 The enforcing authority is also free to raise the grounds of refusal in respect of the Order in its entirety or only in parts.
50 Art. 10(2) and (4) of the Regulation.
51 See also below III.1 h).
52 While the enforcing authority may invoke all the reasons contained in Art. 16(4) and (5), the addressees cannot invoke the reason for a manifest breach of fundamental rights provided for in Art. 16(4)(g) and Art. 16(5)(f), respectively.
53 Cf. Art. 1(3) of the Regulation.
54 Cf. Recital 16 of the Regulation.
55 Art. 13(3) of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *O.J.* L 119, 4.5.2016, 89.
56 Cf. below under III.1. h).
57 Cf. Art. 18(2) of the Regulation.
58 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *O.J.* L 119, 4.5.2016, 1.
59 The service providers are not liable for prejudices to their users or third parties if they act in good faith when complying with the requirements of the European Production Order or the European Preservation Order.
60 It should be asked whether delays in the development of the decentralised IT system could constitute such exceptional circumstances.
61 Regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *O.J.* L 257, 28,8.2014, 73.
62 Art. 9(2) and (3) of the Regulation provides that the EPOC and the EPOC-PR, respectively, be sent to the service providers containing neither information on necessity and proportionality nor a description of the case.
63 Art. 27 of the Regulation. To this end, Member States have to indicate such a decision in a written declaration submitted to the Commission. The Commission will then make the declarations available to all Member States and to the European Judicial Network.
64 Opinion of the Legal Research Service of the German Bundestag of 7 February 2011 in the context of data retention ("Die Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta"), WD 11 – 3000 – 12/11.
65 Art. 1(1) of the Directive.
66 Cf. point 2 in the Explanatory Memorandum of the Commission proposal, COM(2018) 226 final, *op. cit.* (n. 4).
67 Art. 2(1)-(3) of the Directive. See also above under III.1.a).
68 "Established in the Union" in this context means that there is an entity in the Union that pursues an economic activity for an indefinite period of time through a stable infrastructure from which the business of providing services is carried out or the business is managed, cf. Art. 2(4) of the Directive.
69 Situations in which a service provider is established in a Member State and offers services exclusively on the territory of that Member State fall out of the scope of the Directive. Cf. Art. 1(5) of the Directive.
70 Art. 2(3) of the Directive. Cf. to this end also III.1.a) above.
71 Recital 13 of the Directive.
72 *Ibid*.
73 *Ibid*.
74 Recital 17 of the Directive.
75 Cf. Recital 7 of the Directive.
76 Cf. Recital 33 of Directive 2014/41/EU regarding the European Investigation Order in criminal matters, *O.J.* L 130, 1.5.2014, 1.
77 Convention established by the Council in accordance with Article 34 of the Treaty on the European Union on mutual assistance in criminal matters between Member States of the Union, *O.J.* C 197, 12.7.2000, 3.
78 *Ibid*.
79 The Directive does not prevent national authorities of a Member State from continuing to address service providers established on their territory for the purpose of gathering electronic evidence in criminal proceedings in purely domestic situations. However, this should not lead to a circumvention of the principles set out in Directive and the Regulation. Cf. Recital 9 of the Directive.
80 This applies to the service providers that will begin offering services once the Directive has been transposed and in place for more than six months. Cf. Recital 7 of the Directive.
81 Recital 17 of the Directive states that the languages to be used should in any case include one or more of the official languages of the Member State in which the designated establishment is established or the legal representative resides. It may also include other official languages of the Union, such as the language of the headquarters of the service provider.

82 For instance, in the case in which the service provider designates several designated establishments or legal representatives. The territory of all the Member States taking part in the instruments within the scope of this Directive should, however, be covered without leaving any gaps. Cf. Recital 17 of the Directive.
83 Art 3(5) of the Directive
84 Recital 18 of the Directive.
85 Cf. Art. 6(3) and Recital 21 of the Directive.
86 See, for example, the open letter of 25 organisations, ranging from the Council of Bars and Law Societies of Europe (CCBE) to internet service providers, media, and journalist associations: <https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2021_05_18_EevidenceJointLetter_18May2021.pdf>.
87 The most prominent example is the Digital Services Act: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), *O.J.* L 277, 27.10.2022, p. 1.
88 Art. 13(3) of Directive (EU) 2016/680 stipulates that "Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to: (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others."
89 eEvidence: After 5 years of debate European Parliament greenlights agreement | EBU <https://www.ebu.ch/news/2023/06/eevidence-after-5-years-of-debate-european-parliament-greenlights-agreement> accessed 18 September 2023.
90 See also: A. Juszczak and E. Sason. "Recalibrating Data Retention in the EU", (2021) *eucrim,* 238–266.
91 Art. 25 of the Regulation.
92 Agreement on mutual legal assistance between the European Union and the United States of America; *O.J.* L 181, 19.7.2003, 32.
93 The Stored Communications Act (SCA), 18 U.S.C. §§ 2701 *et seq.* governs access to stored wire and electronic communications, such as emails and other online messages held by service providers. It forms part of Title II of the Electronic Communications Privacy Act of 1986 (ECPA).
94 18 U.S.C. Chapter 119 – Wire and electronic communications interception and interception of oral communications § 2523. Executive agreements on access to data by foreign governments.
95 Landmark U.S.-UK Data Access Agreement Enters into Force | OPA | Department of Justice <https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force>.
96 United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime | OPA | Department of Justice <https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime>.
97 United States and Canada Welcome Negotiations of a CLOUD Act Agreement | OPA | Department of Justice <https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement>.
98 COM(2019) 70 final; Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Council document 10128/19 of 2019-06-12; Addendum to the Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Council document 10128 ADD 1/19 of 2019-06-12.
99 Addendum to the Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Council document 10128 ADD 1/19 of 2019-06-12; section 3 point 5 (a bis) and (d).
100 EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations (europa.eu) <https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en>.
101 Addendum to the Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Council document 10128 ADD 1/19 of 2019-06-12, paragraph 9 of section II ("nature and scope of the agreement").
102 Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework. C(2023)4745 final.
103 This includes, for example, the EU Data Act for which political agreement was reached on 28 June 2023 as well as the development of the EU Cybersecurity Certification Scheme on Cloud Services (EUCS).
104 Refer to: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.
105 Explanatory Report to the Convention on Cybercrime, <https://rm.coe.int/16800cce5b>, para. 16.
106 European Council conclusions, 18 October 2018 - Consilium (europa.eu) <https://europa.eu/!gV64YY>.
107 Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM(2019) 71 final.
108 See <https://data.consilium.europa.eu/doc/document/ST-9116-2019-INIT/en/pdf>.
109 Addendum to the Recommendation for a Council Decision authorising the European Commission to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), 27 May 2019, doc. 9664/19.
110 Access to e-evidence: Council authorises member states to sign international agreement – Consilium (europa.eu) <https://europa.eu/!bhYCyR>.
111 See <https://www.coe.int/en/web/cybercrime/second-additional-protocol>; Malta became the 39th State to sign the protocol on 22 June 2023.
112 Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General <https://digitallibrary.un.org/record/1327693?ln=en>.
113 The Russian Federation is excluded from the Council of Europe: <https://www.coe.int/en/web/cpt/-/the-russian-federation-is-excluded-from-the-council-of-europe>.
114 Press review: Russia unveils bid to fight cyber crime and Samsung Pay faces patent issue – TASS <https://tass.com/pressreview/1320973>.
115 United Nations General Assembly, Seventy-fourth session, agenda item 107, Report of the Third Committee, docu-

ment A/74/401, N1938343.pdf (un.org) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/383/43/pdf/N1938343.pdf?OpenElement>.
116 General Assembly Resolution 74/247.
117 General Assembly Resolution 75/282.
118 Structure of the comprehensive international convention on countering the use of information and communications technologies for criminal purposes, as contained in Annex II to document A/AC.291/7.
119 Recommendation for a Council Decision authorising the negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, COM(2022) 132 final.
120 Council Decision (EU) 2022/895.
121 *Ibid*. Negotiating directive 27.
122 Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/222/255/1E/PDF/2222551E.pdf?OpenElement> and <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/039/51/PDF/V2303951.pdf?OpenElement>.
123 Most recently, the EU Statement on Article 36 – Protection of personal data (unodc.org) <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Informals/Coordinators/230901_EU_statement_on_Art._36.pdf>.
124 Available at: <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf>.
125 These costs are estimated by Cybersecurity Venture; the 2022 Official Cybercrime Report is accessible at: <https://www.esentire.com/resources/library/2022-official-cybercrime-report>.
126 Germany, Croatia, Hungary, Poland, and Finland issued an official statement with the adoption of the legislative act. Germany supported the adoption of the Regulation but regretted the lack of clarity as regards the ground for refusal in case of a manifest breach of a fundamental right set out in Art. 6 TEU and in the Charter of Fundamental Rights of the EU and the corresponding recital. Germany also expressed the need for more comprehensive effective remedies, in particular in relation to European Preservation Orders. It also sees a general need to allow for effective remedies not only in the issuing Member State but also in the enforcing Member State. Germany further noted that it considers Recital 53 on the "residence criterion" too vague, particularly the wording on the intention of a person to establish the habitual centre of its interests in a particular Member State as a relevant objective circumstance to determine his/her residence; the wording leaves too much room for interpretation and thus extends the scope of this criterion. Hungary and Poland objected to the inclusion of Art. 7(1) TEU in a recital related to the ground for refusal of European Production Orders in case of a manifest breach of a fundamental right set out in Art. 6 TEU and in the Charter of Fundamental Rights of the EU. Although Croatia expressed its dissatisfaction with the linguistic version of the proposals, it generally welcomed the adoption of the legislative acts. Finland voted against the adoption of the Regulation, reasoning that a judicial assessment should also be carried out by the competent authorities in the enforcing State for European Production Orders issued in relation to the most sensitive data. Finland also regretted that the grounds for refusal do not include a ground allowing the enforcing authority to refuse a production order for traffic and content data in cases in which the use of such a measure is restricted under the law of the enforcing State to certain offences or to offences punishable by a certain minimum threshold.

# Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings

Pavlos Topalnakos

**The new EU Regulation on electronic evidence in criminal proceedings not only aims to enhance cross-border access to electronic evidence but also raises concerns regarding privacy, fundamental rights, and accountability. This article focuses on three key issues.**
**First, it is argued that the establishment of a direct cooperation framework between the issuing state and private service providers regarding data of citizens from other Member States reinterprets Art. 82 TFEU and circumvents the traditional review and scrutiny by the judicial authorities of the enforcing state, compromising transparency and individual rights.**
**Second, the rules in the Regulation that eliminate the requirement of dual criminality for certain categories of electronic evidence potentially lead to the collection of data for conducts that may not be criminalized in the enforcing state. In addition, the absence of the principle of speciality allows for the unintended use of evidence acquired through cooperation.**
**Third, the individuals' rights to privacy and data protection are potentially violated, given that European Preservation Orders fall outside the scope of legal remedies. Moreover, the lack of explicit provisions for legal protection within the enforcing state raises concerns about the effectiveness of the remedies.**
**The author stresses the need to strike a balance between deepening cooperation and safeguarding fundamental freedoms. He calls for reforms to ensure robust mechanisms for contesting the legality and necessity of measures, as well as clear provisions for legal protection within the enforcing state, so that a rights-based approach within the European system established by the Regulation can be achieved.**

## I. Introduction

The general objective of effective investigation and prosecution of crimes has always been an essential dimension of judicial cooperation in criminal matters within the EU. In the era of technological advancement, efficient judicial cooperation must include the improvement of cross-border access to electronic evidence. This improvement was initially pursued by Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order (EIO) in criminal matters.[1] However, the collection of electronic evidence through the EIO only focused on the identification of individuals who were associated with a specific telephone number or IP address[2] and on the interception of telecommunications with the technical assistance of the executing state[3]. As a result, it became quickly apparent that the EIO fell short of the set targets, because the procedures and timelines prescribed in the EIO proved unsuitable for electronic information,[4] which is more volatile and subject to swift and easy deletion.

In this context, three new objectives were set: [5]

- Reducing delays in cross-border access to electronic evidence;
- Ensuring cross-border access to evidence where it is currently missing by means of the EIO;
- Improving legal certainty, protection of fundamental rights, transparency, and accountability.

With this perspective in mind, and after a rather laborious process, final agreement was reached on the European Production Order and the European Preservation Order for electronic evidence in criminal proceedings.[6] This article will highlight three specific issues that are considered key in the Regulation: First, the new function seemingly attributed to Art. 82 of the Treaty on the Functioning of the European Union (TFEU) that regulates the judicial cooperation of Member States in criminal matters within the EU. Second, the application of fundamental principles that traditionally govern judicial cooperation between states. Third, the legal remedies provided to the individuals who are affected by the issued Orders.

## II. A New, Previously Unknown Function of Article 82 TFEU

The activation of Art. 82 TFEU in all cases where it was invoked as the legal basis for mutual cooperation between EU Member States led to the establishment of a stable framework involving two judicial authorities: those of the issuing state and those of the executing state. The new Regulation on electronic evidence changes this framework for the sake of a speedy collection of evidentiary material, bypassing the judicial authorities of the enforcing state and allowing direct cooperation between the competent authorities of the state issuing the European Production and Preservation Order and the private sector service providers. In essence, this process allows the authorities of the issuing state to gain direct access to a range of data concerning citizens of other Member States without being subject to scrutiny by the judicial authorities of the enforcing state regarding the conditions for issuing and the overall legitimacy of said Orders. It is worth emphasizing that the granted access may even cover sensitive personal data,[7] while the power of review lies primarily with the service providers, who, obviously, cannot guarantee the protection of the rights of the individuals affected by these Orders. Moreover, the protection of rights becomes even more precarious when two additional factors are taken into account: First, the execution time for the Orders is relatively short and tight, making it practically impossible to thoroughly verify the adequacy and legitimacy of said Orders.[8] Second, the threat against service providers of pecuniary sanctions for infringements of the Regulation undoubtedly undermines the "will" to scrutinize the legitimacy of the Orders, as it is rather apparent that the service provider would prefer an "easy" compliance with the Orders over being subjected to the looming threat of pecuniary sanctions.[9]

The Regulation seeks to address these weaknesses by establishing, in its Art. 8, the obligation of the issuing state to inform the competent authority of the enforcing state simultaneously with the transmission of the certificate issued for the Order. However, this notification only concerns the issuance of a European Production Order, not the issuance of a European Preservation Order, and it is furthermore limited to cases where the data submitted are traffic and content data. On the contrary, cases involving data used for the sole purpose of identifying the user and subscriber data do not require notification of the enforcing state.

The characteristics of the new Regulation on European Production and Preservation Orders as described make it clear that the framework established by it, with Art. 82 TFEU as its legal basis, has fundamentally altered the essence of this provision of EU primary law, which aims to facilitate the judicial cooperation between states guided by principles of review and transparency and not between states and private entities, where critical factors, such as mutual recognition, are lacking.

## III. The Principle of Dual Criminality and the Principle of Speciality

No matter how much it may facilitate the judicial cooperation between states sidelining the principles that traditionally govern such cooperation, the abandonment of the dual criminality principle remains a choice that carries a serious risk: The service provider with a designated establishment or legal representative in the enforcing state will be obliged to contribute to the punishment of a conduct that would go unpunished in the territory of the enforcing state. This may result in imposing burdensome measures on individuals that the competent authorities of the enforcing state would not be able to take if the same conduct had occurred within their jurisdiction.

The Regulation on European Production and Preservation Orders does not really mitigate this risk. The provision of Art. 12 para. 1 (d), which, in combination with Art. 8 of the Regulation, stipulates as a ground for refusal of a European Production Order the non-criminalization of the conduct in the enforcing state, was intended to limit the aforementioned risk. However, it is accompanied by the classic exception of a list of offenses for which the dual criminality requirement is not necessary when the issuing state provides for a maximum penalty exceeding three years. Except for that, the principle of dual criminality only applies in cases where two specific categories of electronic evidence are requested: traffic data and content data. As a result, the restriction of dual criminality does not apply in cases of data requested for the sole purpose of identifying the user and subscriber data. Therefore, the aforementioned risk of producing and preserving these particular categories of data for conducts that do not constitute an offense in the enforcing state still remains more than real. Furthermore, there is no provision regarding the application of the dual criminality principle in cases of European Preservation Orders, regardless of whether they concern subscriber data, data requested for the sole purpose of identifying the user, traffic data, or content data; this is based on the thought that electronic evidence under European Preservation Orders does not result in the disclosure of the aforementioned data.[10] According to this argument, a European Preservation Order constitutes a prerequisite for the issuance of the European Production Order, which is subject to the aforementioned review of the principle of dual criminality, so the examination of the dual criminality principle will be carried out at a later stage.

The tendency to bypass the principles that traditionally govern the field of judicial cooperation in criminal matters is highlighted by the complete abandonment of the principle of speciality, which had already been set aside by the Directive regarding the European Investigation Order.[11] Thus, evidence electronically acquired through cooperation between Member States in criminal matters can apparently be used for purposes other than those for which cooperation was sought, leaving the door wide open for the evidentiary exploitation of inadvertent findings.

## IV. Remedies Available to Individuals Involved in the European Production and Preservation Orders

Legal safeguards for individuals whose data are collected, irrespective of whether they are suspects, defendants, or third parties, seem to be primarily confined to cases of European Production Orders. These legal remedies are provided by the state issuing the Order, and the individuals concerned can contest the legitimacy, necessity, and proportionality of the measures before the competent authorities of the issuing state. Therefore, electronic evidence collected under a European Preservation Order remains outside the scope of legal remedies on the grounds that it alone does not result in the disclosure of data and after all, if the issuance of the European Production Order follows, then the review can be carried out within the framework referred to in Art. 18 of the Regulation. However, it should not be overlooked that the service provider may have an obligation under its domestic legislation to delete or restrict the processing of data for which the retention was requested through the European Preservation Order. Therefore, the retention of data under the European Preservation Order that should have been deleted or where processing should at least be restricted leads to a violation of the rights of the individuals regarding the protection of their personal data and their private and family life. And all of this at a time when the retention period of the data by the service provider can be extended from the initial sixty days period by an additional thirty days (Art. 11 para. 1), and then for an indefinite period, until the European Production Order is issued or revoked, without any upper limit on the retention of such data.

Moreover, the absence of an explicit provision guaranteeing the exercise of legal remedies within the enforcing state should also be noted, which could create serious issues regarding the effectiveness of the legal protection provided, since the persons concerned would have to resort to the issuing state to exercise their rights, which is inherently challenging. However, the addition made in Art. 18 para. 2 *in finem* of the Regulation regarding the guarantees of fundamental rights in the enforcing state should not only serve as a semantic safeguard but should also be considered to have regulatory content that includes the review of the Or-

der by the enforcing state when requested by the person concerned, as provided in the domestic law for the same cases.

## V. Conclusion

This article raised three cutting-edge issues of the new Regulation on electronic evidence in criminal matters, as they touch upon the most sensitive aspects of mutual judicial cooperation within the EU: the legal basis of the Regulation, fundamental principles of interstate cooperation, and protection of rights / effective remedies for the individuals concerned. While judicial cooperation between Member States appears to be deepening and taking new forms, it seems to be happening at the expense of rights and principles safeguarding the fundamental freedoms of individuals. The deepening of this cooperation does not serve as an end in itself but is only meaningful if it serves the freedoms of individuals. And this cannot be sidelined. In conclusion, efforts should be made to ensure that legal safeguards are in place to protect the rights of individuals subject to the European Production and Preservation Orders, including robust mechanisms for contesting the legality and necessity of measures, as well as clear provisions for legal protection within the enforcing state. Such reforms would contribute to a more balanced and rights-based approach within the system established by the Regulation.

1 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order in criminal matters, *O.J.* L 130, 1.5.2014, 1.
2 Art. 10(2) (e) of the EIO Directive, *op. cit.* (n. 1).
3 Art. 30 of the EIO Directive, *op. cit.* (n. 1).
4 Arts. 12(3) and (4) of the EIO Directive, *op. cit.* (n. 1), where the executing authority in the European Investigation Order has a deadline of 30 days to recognize the request and must execute the order within 90 days.
5 See Commission Staff Working Document Impact Assessment accompanying the document "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings", SWD (2018) 118 final, table 5, p. 41.
6 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *O.J.* L 191, 28.7.2023, 118–180.
7 Art. 9 of the General Data Protection Regulation, *O.J.* L 119, 4.5.2016, 38.

**Pavlos Topalnakos, Dr. jur.**
**Lawyer**

8 The addressee is obliged to execute the order – meaning to transmit the data within 10 days or within 8 hours in case of emergency, see Art. 10 of the Regulation, *op. cit.* (n. 6).
9 Art. 15 of the Regulation, *op. cit.* (n. 6).
10 The Explanatory Memorandum of the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, reads as follows at p. 22: "Given that the European Preservation Order itself does not result in data disclosure and therefore does not give rise to similar concerns, the review procedure is limited to the European Production Order".
11 Regarding this principle, see Arts. 27(2) and (3) of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant, *O.J.* L 190, 18.07.2002, 1.

# Preuves électroniques : état de la situation en Suisse face à l'avancée majeure du droit européen

Maria Ludwiczak Glassey

**This contribution is a comparison of the solution adopted in the European Union (EU) concerning cross-border access to electronic evidence and the Swiss law applicable in this area, based on a number of key features of the European system. It gives rise to a reflection on the prospects for relations between the European Union and Switzerland, in particular the opportunity for Switzerland to coordinate its rules with those of European law.**

## I. Introduction

L'aboutissement, en juillet 2023, du projet *e-Evidence* représente un pas fondamental dans la modernisation de l'accès transfrontalier aux preuves électroniques au sein de l'Union européenne. En effet, l'adoption du Règlement (UE) 2023/1543 du 12 juillet 2023 relatif aux injonctions européennes de production et de conservation concernant les preuves électroniques dans le cadre des procédures pénales[1] (ci-après : Règlement *e-Evidence*) et de la Directive (UE) 2023/1544 du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales[2] (ci-après : Directive *e-Evidence*) permet une adaptation de l'accès transfrontalier aux preuves, compte tenu de la nature dématérialisée des données. Cela crée une cohérence entre la nature des données et le processus à disposition des autorités de poursuite pénale des États membres de l'UE pour les obtenir.[3]

La présente contribution se propose de comparer, sur la base de quelques traits majeurs du système *e-Evidence*, la solution novatrice retenue dans l'Union véhiculée par le système *e-Evidence* et le droit suisse applicable en l'état à la matière :[4] la surveillance de la correspondance par télécommunications relevant du droit de la procédure pénale suisse, c'est-à-dire les art. 269 ss CPP[5] et la LSCPT[6].

Afin de limiter le champ de la contribution, ne sera abordée que la question de la production des preuves électroniques par le biais de l'injonction européenne de production (*European Production Order*, EPO), celle portant sur la conservation étant mise de côté. Par ailleurs, ne sera pas traitée la question de la surveillance en temps réel, celle-ci ne faisant pas partie du champ du système *e-Evidence* (art. 3 par. 8 Règlement *e-Evidence* : « données [...] stockées par un fournisseur [...] au moment de la réception d'un certificat »). Finalement, nous nous concentrerons sur les données électroniques requises au titre de moyens de preuve dans le cadre d'une procédure pénale en cours et pas pour l'exécution d'une sanction déjà prononcée, bien que ces cas de figure soient également couverts par le système *e-Evidence* (voir déjà l'intitulé du Règlement *e-Evidence*).

## II. Quelques points de comparaison

Seront développés dans les lignes qui suivent quelques aspects essentiels du système *e-Evidence* permettant d'opérer une comparaison, non exhaustive, avec le droit suisse actuellement en vigueur régissant la transmission des preuves en format numérique pour les besoins d'une procédure pénale. Ainsi, seront traités tour à tour le type de données concernées et leur lieu de stockage physique (1.), la détermination du fournisseur de services astreint à l'obligation de fournir les données et la portée extraterritoriale de cette obligation (2.), le seuil de gravité des faits à partir duquel le système est applicable (3.), les modalités de contact avec le fournisseur de services (4.) et l'étendue de l'obligation de fournir les données (5.).

### 1. Données concernées et lieu de stockage

Le système *e-Evidence* concerne les « preuves électroniques », par quoi il faut entendre les données relatives aux abonnés, au trafic et au contenu stockées sous une forme numérique par un fournisseur de services ou pour le compte d'un tel fournisseur (art. 3 par. 8 Règlement *e-Evidence*). Les données relatives aux abonnés sont celles concernant l'identité d'un abonné ou d'un client (nom, date de naissance, adresse), les données de facturation et de paiement, le numéro de téléphone et l'adresse électronique fournis, mais

aussi notamment les données relatives au type de service et à sa durée (art. 3 par. 9 Règlement *e-Evidence*). Certaines données, tels les adresses *IP* et les ports de provenance et l'horodatage pertinents, peuvent être demandées à la seule fin d'identifier l'utilisateur (art. 3 par. 10 Règlement *e-Evidence*) et seront alors assimilées aux données relatives aux abonnés. Les données relatives au trafic sont celles qui concernent la fourniture d'un service proposé par le fournisseur, tels par exemple la source et la destination d'un message, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé, le type de compression, etc. (art. 3 par. 11 Règlement *e-Evidence*). Finalement, les données relatives au contenu sont toutes les données dans un format numérique (texte, voix, vidéos, images et son) qui ne sont relatives ni aux abonnés ni au trafic (art. 3 par. 12 Règlement *e-Evidence*). Selon le type de données, des régimes différenciés sont prévus, notamment en fonction du seuil de gravité des faits et s'agissant de la question de savoir si l'intervention d'une autorité judiciaire est nécessaire (*infra* II.3. et II.4.b).

Le droit suisse établit également une distinction entre les types de données concernées, mais ne connait que deux catégories, à savoir les données relatives au contenu, d'une part, et les données dites secondaires (ou métadonnées) visant l'identification, la localisation et les caractéristiques techniques de la correspondance[7], d'autre part. Les données secondaires au sens du droit suisse regroupent ainsi les données relatives aux abonnés, les données demandées à la seule fin d'identifier l'utilisateur et les données relatives au trafic désignées par le système *e-Evidence*. Les différences entre les régimes applicables sont moindres qu'en droit européen (*infra* II.3. et II.4.b).

Le système *e-Evidence* se caractérise par l'abandon du critère de la localisation des données. En d'autres termes, le lieu de stockage physique, c'est-à-dire l'endroit où se trouve le *data center* où les données sont enregistrées, n'est pas pertinent. Ainsi, que les données soient physiquement stockées dans un (ou plusieurs) État(s) de l'UE ou dans un État tiers n'a aucune pertinence. De même, le droit de la procédure pénale suisse, tel qu'interprété par le Tribunal fédéral suisse, permet l'accès des autorités suisses à des données stockées à l'étranger.[8] La possibilité de perquisitionner le *data center*, lorsqu'il se trouve sur le sol suisse est réservée (art. 244 ss CPP), tout comme celle, pour les autorités de poursuite des États de l'UE, de faire usage de leurs règles de procédure pénale interne pour accéder aux données physiquement localisées sur leurs territoires respectifs. Selon notre compréhension, le système *e-Evidence* permet à l'autorité de poursuite pénale d'un État de l'UE de choisir entre une perquisition et une EPO si le *data center* se trouve sur son territoire, mais que le fournisseur est rattaché à un autre État de l'UE.

## 2. Fournisseur de services concerné

### a) Notion de fournisseur de services

Tel qu'exposé ci-dessus, le critère permettant l'application du système *e-Evidence* ne réside pas dans la localisation des données dans un État membre de l'UE, respectivement en Suisse pour la surveillance de la correspondance par télécommunications. Il est lié au fait qu'un fournisseur propose des services électroniques dans l'Union, respectivement est soumis au droit suisse.

Au sens du Règlement *e-Evidence* (art. 3 par. 3 Règlement *e-Evidence*), est considéré comme un fournisseur de services toute personne physique ou morale qui fournit des services de communications électroniques[9]. Il s'agit des **services d'attribution de noms de domaine** sur l'internet et de numérotation *IP* et d'autres services de la société de l'information[10] qui permettent à leurs utilisateurs de **communiquer** entre eux, de **stocker** ou de **traiter** d'une autre manière des données pour le compte des utilisateurs auxquels le service est fourni, à condition que le stockage des données soit une composante déterminante du service fourni à l'utilisateur. Sont expressément exclus les services financiers tels que ceux ayant trait à la banque, au crédit, à l'assurance et à la réassurance, aux retraites professionnelles ou individuelles, aux titres, aux fonds d'investissements, aux paiements et aux conseils en investissement (art. 3 par. 3 Règlement *e-Evidence* renvoyant à l'art. 2 par. 2 let. b Directive 2006/123/CE du 12 décembre 2006 relative aux services dans le marché intérieur).

Il n'est pas pertinent de savoir si le fournisseur est **établi ou non dans l'UE**, étant précisé que par établissement on entend une entité qui exerce de manière effective une activité économique pendant une durée indéterminée au moyen d'une infrastructure stable à partir de laquelle l'activité de fourniture de services est réalisée ou gérée (art. 2 par. 4 et art. 3 par. 5 Directive *e-Evidence*). Concrètement, si un fournisseur est établi dans un État de l'UE qui participe au système *e-Evidence*, cet État devra veiller à ce que ce fournisseur désigne le (ou les) établissement(s) qui sera (seront) le point de contact pour les autorités pénales (art. 3 par. 1 let. a Directive *e-Evidence*) ; si tel n'est pas le cas, c'est aux États membres sur les territoires desquels le fournisseur propose ses services qu'il incombe d'y veiller (art. 3 par.1 let. b Directive *e-Evidence*).

Selon le droit suisse, sont concernés les fournisseurs de services de télécommunication, notion qui a une portée

large.[11] Est déterminante la transmission d'informations pour le compte de tiers au moyen de techniques de télécommunication.[12] Sont visés en particulier les fournisseurs d'accès à Internet, soit tout fournisseur de services de télécommunication qui offre une prestation publique de transmission d'informations sur la base de la technologie *IP* et d'adresses *IP*, mais aussi les fournisseurs de services de télécommunication et les services de communication dérivés. Selon le Conseil fédéral suisse, cela comprend notamment les fournisseurs de services Internet qui permettent une communication unilatérale rendant possible le chargement de documents, ceux qui permettent une communication multilatérale rendant possible la communication entre usagers, les fournisseurs d'espaces de stockage d'e-mails, les fournisseurs d'hébergement d'applications ou services email, les fournisseurs d'hébergement y compris de type « *cloud* », les plates-formes de *chat*, les plates-formes d'échange de données et les fournisseurs de services de téléphonie par Internet.[13]

#### b) Caractéristiques des fournisseurs de service visés

Tout fournisseur de services électroniques n'est toutefois pas concerné. Le critère choisi dans le système *e-Evidence* est le fait de proposer des services dans l'Union, pendant qu'il s'agit, selon le système suisse, du fait d'être soumis au droit suisse, d'une part, et du contrôle des données, d'autre part. Les critères choisis dans les deux systèmes sont ainsi différents. Des précisions s'imposent sur ces notions.

Proposer des services dans l'UE se définit comme permettre aux personnes physiques ou morales dans un État membre d'**utiliser les services** et avoir un **lien substantiel**, fondé sur des critères factuels spécifiques, avec ledit État membre. Un tel lien substantiel est réputé exister lorsque le fournisseur de services dispose d'un établissement dans un État membre ou lorsqu'il existe un nombre significatif d'utilisateurs dans un ou plusieurs États membres ou lorsqu'il existe un ciblage des activités sur un ou plusieurs États membres (art. 3 par. 4 Règlement *e-Evidence*).

Le fait d'être **soumis au droit suisse** est une notion juridique impliquant que l'entité dispose de droits et est astreinte à des devoirs imposés par le droit suisse. Ainsi, une société dont le siège se trouve en Suisse remplit cette condition. Il en est de même de la filiale suisse d'un fournisseur de services étranger. La jurisprudence suisse exige un critère supplémentaire à savoir le fait que l'entité soumise au droit suisse (et non par exemple la maison mère en cas de filiale en Suisse) doit avoir un **contrôle sur les données à produire**, ce par quoi il faut entendre « un pouvoir de disposition, en fait et en droit, sur ces données »[14].

Il sied encore de préciser que sont exclus du système *e-Evidence* les cas dans lesquels une procédure pénale est conduite dans un État membre de l'UE et que le fournisseur déploie ses activités dans ce même État membre. En effet, le système a une vocation extraterritoriale et est ainsi sans préjudice des pouvoirs des autorités nationales de s'adresser aux fournisseurs de services établis ou représentés sur leur territoire afin qu'ils se conforment à des mesures nationales similaires (art. 1 par. 1 al. 2 Règlement *e-Evidence*). Le droit suisse, applicable au seul État suisse, ne connait par la force des choses pas cette distinction.

### 3. Seuil de gravité des faits

Un seuil de gravité des faits est prévu dans les deux systèmes. En droit de l'UE, l'EPO est soumise aux principes de nécessité et de proportionnalité (art. 5 par. 2 Règlement *e-Evidence*). Une distinction est faite selon si les données sont relatives aux abonnés ou demandées aux seules fins d'identifier une personne, d'une part, ou si elles sont relatives au trafic ou au contenu, d'autre part. Ainsi, une EPO est possible dans le premier cas pour **toutes les infractions pénales** (art. 5 par. 3 Règlement *e-Evidence*). Dans le second cas, une EPO est possible uniquement pour des infractions punissables dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'**au moins trois ans** (art. 5 par. 4 let. a Règlement *e-Evidence*), pour certaines infractions totalement ou partiellement commises au moyen d'un système d'information (art. 5 par. 4 let. b Règlement *e-Evidence*) et pour certaines infractions terroristes (art. 5 par. 4 let. c Règlement *e-Evidence* renvoyant à la Directive (UE) 2017/541 du 15 mars 2017 relative à la lutte contre le terrorisme).

En droit suisse également, la surveillance de la correspondance par télécommunications est conditionnée par les principes de nécessité (art. 269 al. 1 let. c CPP) et de proportionnalité (art. 269 al. 1 let. a et b CPP) et une distinction est opérée en fonction de la nature des données. S'agissant des données secondaires (c'est-à-dire relatives aux abonnés et au trafic), l'obtention des preuves électroniques est possible pour **tous les crimes et les délits** (art. 263 al. 1 CPP), donc les infractions passibles d'une peine privative de liberté de plus de trois ans (crimes au sens de l'art. 10 al. 2 CP[15]), respectivement d'une peine privative de liberté n'excédant pas trois ans ou d'une peine pécuniaire (délits au sens de l'art. 10 al. 3 *cum* 34 et 40 CP). Le droit suisse se montre ainsi plus limitatif que le droit de l'UE s'agissant des données secondaires, qui ne pourront être obtenues pour des contraventions (passibles uniquement d'une amende, art. 103 *cum* 106 al. 1 CP).

L'obtention des données relatives au contenu est, quant à elle, limitée à un (long) catalogue d'infractions énumérées ex-

haustivement dans la loi (art. 269 al. 2 CPP), parmi lesquelles ne se trouvent que les **infractions les plus graves**, crimes et délit confondus. À titre d'exemples, parmi les infractions dirigées contre la vie, ne font pas partie du catalogue les délits que sont le meurtre sur la demande de la victime (art. 114 CP), l'infanticide au sens de l'article 116 CP, l'homicide par négligence (art. 117 CP) et l'interruption de grossesse punissable avec le consentement de la mère (art. 118 ch. 1 CP), alors que d'autres formes d'homicide sont listées (meurtre, art. 111 CP ; assassinat, art. 112 CP ; meurtre passionnel, art. 113 CP ; incitation et assistance au suicide, art. 115 CP ; interruption de grossesse punissable sans le consentement de la mère (art. 118 ch. 2 CP). Le droit suisse peut être considéré comme plus restrictif, en ce sens que les données relatives au contenu ne peuvent pas être obtenues pour certaines infractions passibles, selon le droit suisse, d'une peine privative de liberté de plus de trois ans (p. ex. l'interruption de grossesse punissable avec le consentement de la femme enceinte, passible d'une peine privative de liberté de cinq ans au plus, art. 119 al. 1 CP).

## 4. Modalités de contact avec le fournisseur de services par l'autorité de poursuite pénale

### a) Accès (in)direct au fournisseur de services

Le système *e-Evidence* repose sur un **accès direct** au fournisseur de services par l'autorité de poursuite pénale (art. 7 par. 1 Règlement *e-Evidence*).[16]. À cette fin, pour tenir compte de la multiplicité des États concernés, chaque fournisseur de services est tenu d'indiquer un établissement désigné ou annoncer un représentant légal qui sera son point de contact (art. 3 Directive *e-Evidence*). Lorsque plusieurs établissements ou représentants légaux sont désignés, leurs compétences respectives en particulier la portée territoriale de leurs attributions, doivent être clairement énoncées (art. 4 par. 3 Directive *e-Evidence*). Les autorités pénales des États membres s'adressent ainsi directement au représentant légal ou à l'établissement désigné se trouvant dans un autre État membre au moyen du certificat d'injonction européenne de production (*European Production Order Certificate*, EPOC, art. 9 et Annexe I Règlement *e-Evidence*).[17] Lorsque les données requises sont relatives au trafic ou au contenu, l'EPOC est, en principe, adressé parallèlement à l'autorité chargée de la mise en œuvre (art. 8 par. 1 Règlement *e-Evidence*).[18]

Le droit suisse quant à lui ne permet pas d'accès direct par les autorités pénales suisses aux fournisseurs de services électroniques. Les autorités pénales sont tenues de s'adresser, au moyen d'un formulaire, au Service Surveillance de la correspondance par poste et télécommunication (Service SCPT, art. 3 al. 1 LSCPT) qui est chargé de recueillir les données auprès des fournisseurs puis de les transmettre à l'autorité de poursuite (art. 15 al. 1 LSCPT). Chaque fournisseur est tenu de désigner un service responsable de la surveillance et de la fourniture de renseignement auquel le Service SCPT adressera les demandes (art. 5 al. 1 *cum* 4 al. 1 OME-SCPT[19]).

### b) Intervention d'une autorité judiciaire

S'agissant de la question de savoir si l'injonction de production peut être émise par un procureur sans l'intervention d'une autorité judiciaire, le système *e-Evidence* fait une distinction selon si les données sont relatives aux abonnés ou visent à identifier une personne, d'une part, ou si elles sont relatives au trafic ou au contenu, d'autre part. Une validation par une autorité judiciaire de l'État d'émission n'est nécessaire que dans le second cas (art. 4 par. 1 let. a et art. 4 par. 2 let. a Règlement *e-Evidence*, respectivement). Les règles de procédure pénale de l'État d'émission sont alors applicables.

Le droit de la procédure suisse exige quant à lui que toute surveillance de la correspondance par télécommunication, qu'elle porte sur des données relatives aux abonnés, au trafic ou au contenu, soit validée par une autorité judiciaire, à savoir le Tribunal des mesures de contrainte (TMC ; art. 272 al. 1 et 273 al. 2 CPP). La procédure se fait en deux temps : l'autorité de poursuite ordonne la mesure et l'adresse au Service SCPT, puis dispose de 24 heures pour transmettre sa demande au TMC (art. 274 al. 1 CPP), qui statue dans les cinq jours (art. 274 al. 2 CPP) et communique sa décision tant à l'autorité de poursuite qu'au Service SCPT (art. 274 al. 3 CPP). En ce qui concerne les données secondaires, le droit suisse est ainsi plus strict sous cet angle que le droit européen.

## 5. Obligation de fournir les données et possibilité de refus

Le système *e-Evidence* prévoit que l'établissement désigné ou le représentant légal du fournisseur concerné (voir *supra* II.2.b) est le point de contact compétent pour la réception, le respect et l'exécution des EPO (art. 3 par. 1 Directive *e-Evidence* ; art. 7 par. 1 Règlement *e-Evidence*). Il est soumis à l'obligation de fournir les données directement à l'autorité de poursuite pénale d'un autre État membre, sous la menace de procédures de mise en œuvre et de sanctions (art. 7 ss Règlement *e-Evidence*). Des motifs de refus d'EPO sont prévus à l'art. 12 Règlement *e-Evidence*, mais ils ne sont applicables que si l'EPO est adressé, parallèlement au point de contact du fournisseur, à l'autorité chargée de la mise en œuvre. C'est cette autorité qui pourra alors se prévaloir du motif de refus. En d'autres termes, une EPO ne peut être refusée que s'agissant des données relatives au trafic et au contenu (art. 8 Règlement *e-Evidence*) et pour des raisons très limitées prévues exhaustivement à l'art. 12 du Règlement, que sont

les cas d'immunités et privilèges, la protection de la liberté de la presse, la violation manifeste d'un droit fondamental, le principe *ne bis in idem* et l'absence de double incrimination. Une procédure de prise de contact entre les autorités nationales est alors prévue (art. 12 par. 2 Règlement *e-Evidence*).

En droit suisse, le fournisseur a l'obligation de transmettre les données requises au Service SCPT (art. 21 ss LSCPT) qui lui-même les transmet à l'autorité pénale requérante (art. 17 let. d LSCPT). À la différence du système *e-Evidence*, aucun motif de refus n'est prévu.

## III. L'accès aux preuves électroniques au-delà des frontières de l'UE et perspectives pour la Suisse

Le système *e-Evidence* et l'accès direct au fournisseur de services électroniques qu'il met en place remplace les mécanismes antérieurs prévalant entre les États membres de l'UE participants. Il s'agit d'un système interne à l'UE : il ne permet pas aux autorités pénales d'un État tiers à l'UE, comme la Suisse, de s'adresser directement à l'établissement désigné ou au représentant légal. Il ne permet pas non plus à un État non-membre d'adresser une demande d'entraide à un État membre qui fera usage de l'EPO pour l'exécuter (par. 23 des considérants et art. 2 par. 4 Règlement *e-Evidence*). Ainsi, le système e-Evidence ne remplace pas les règles applicables à la coopération internationale en matière pénale avec les États non-membres de l'Union[20].

Se pose ainsi la question des règles applicables lorsque les autorités d'un État membre de l'UE veulent obtenir des données auxquelles la Suisse a accès, ou *vice versa*. Hormis les instruments classiques de coopération, telle la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 (CEEJ) complétée par ses Protocoles additionnels (dont seul le second est applicable pour la Suisse), la Convention sur la cybercriminalité conclue à Budapest le 23 novembre 2001 (CCC)[21] contient des règles sur l'accès transfrontalier aux preuves électroniques. Le Deuxième Protocole, relatif au renforcement de la coopération et de la divulgation de preuves électroniques, conclu à Strasbourg le 12 mai 2022 (STE 224), permettant un accès direct au fournisseur de services, n'a pas été ratifié par la Suisse. La CCC ne va pas au-delà de ce qui était déjà possible en application du droit suisse pertinent, à savoir la Loi fédérale régissant l'entraide internationale en matière pénale (EIMP)[22], à tout le moins s'agissant de la surveillance rétroactive. Ainsi, lorsque la Suisse reçoit une demande d'entraide portant sur une forme de surveillance de la correspondance par télécommunication, elle appliquera les règles exposées dans la présente contribution (notamment et pour partie par renvoi de l'art. 18*a* EIMP).[23] Par application du principe de la réciprocité, les autorités suisses ne peuvent adresser à un État étranger de demande portant sur des mesures qu'elles ne pourraient pas entreprendre si les rôles étaient inversés (art. 30 al. 1 EIMP). La coopération est soumise aux motifs de refus ordinaires applicables en matière de coopération internationale (notamment principes *ne bis in idem*, double incrimination et proportionnalité), mais elle est surtout chronophage et tributaire de formalités qui ne s'accommodent que très peu des caractéristiques des preuves électroniques.[24]

Afin de pallier ces inconvénients qui peuvent s'avérer rédhibitoires pour la procédure pénale, une possibilité résiderait dans l'association de la Suisse au système européen *e-Evidence*. Ainsi, les autorités de poursuite des États membres de l'UE pourraient avoir accès aux données contrôlées par des fournisseurs suisses (qui ne proposent pas de services dans l'UE) et *vice versa*. Si une volonté politique naît en ce sens, resteront à déterminer les modalités d'une telle avancée, en particulier comment concilier les différences exposées dans la présente contribution, notamment s'agissant de l'accès direct aux représentants des fournisseurs de services possible dans le système *e-Evidence* mais exclue en droit suisse ou les divergences s'agissant des seuils de gravité prévalant dans les deux systèmes.

## IV. Conclusion

Le système *e-Evidence* renverse la logique classique de la coopération internationale en matière pénale entre les États membres. Il fait fi de la localisation physique des données, permet aux autorités de poursuite un accès direct au fournisseur de services sans impliquer ni l'État où les données sont stockées, ni celui où le fournisseur de services est établi, ni la personne concernée par la transmission des preuves en question. En ce sens, il exclut en partie le contrôle sur la transmission et déroge ainsi fondamentalement à la logique souverainiste du droit de la coopération. Il crée un espace européen de procédure pénale en matière d'accès transnational aux preuves électroniques.

La Suisse, bien que disposant des bases légales lui permettant d'accéder aux preuves électroniques situées à l'étranger, a opté pour des critères de rattachement qui restreignent cet accès, en tant qu'ils ne correspondent pas aux réalités concrètes. Les autorités pénales suisses sont ainsi systématiquement amenées à procéder par le biais de la coopération judiciaire internationale classique pour obtenir des données électroniques, voie qui n'est pas adaptée à ce type de données et, plus généralement à la cybercriminalité. Une réflexion doit, à notre avis, être initiée à ce propos.

Cela étant, tant au sein de l'UE qu'en Suisse demeure la question de l'exploitabilité et donc l'admissibilité dans le cadre d'une procédure pénale des moyens de preuve obtenus sur le plan transnational.[25] Éphémères et manipulables par nature, ces données impliquent des précautions particulières pour assurer leur fiabilité. C'est sans doute là un des terrains sur lesquels les juristes, suisses et européens, devront, ensemble on l'espère, réfléchir dans un avenir proche.

**Maria Ludwiczak Glassey**
Prof. Dr. iur., Universités de Genève et Neuchâtel

1 [2023] *JO* L 191/118.
2 [2023] *JO* L 191/181.
3 L'Irlande a exercé son droit de *opt-in* (considérant 100 du Règlement *e-Evidence*) et le Danemark celui d'opt out (considérant 101 du Règlement *e-Evidence*).
4 Pour une comparaison de droits d'autres États, voir U. Sieber / N. von zur Mühlen /T, Tropina (édit.), *Access to Telecommunication Data in Criminal Justice. A Comparative Legal Analysis*, 2e ed., Berlin 2022.
5 Code de procédure pénale suisse du 5 octobre 2007 ; Recueil systématique du droit fédéral suisse 312.0.
6 Loi fédérale sur la surveillance par poste et télécommunications du 18 mars 2016 ; Recueil systématique du droit fédéral suisse 780.1.
7 Voir l'intitulé de l'art. 273 CPP.
8 ATF 143 IV 21, considérant 3.3 ; voir aussi TF, 1B_142/2016, 16 novembre 2016, considérant 3.3.
9 Renvoi est fait ici à l'art. 2 par. 4 de la Directive (UE) 2018/1972 du 11 décembre 2018 établissant le code des communications électroniques européen.
10 Renvoi est fait ici à l'art. 1 par. 1 let. b, de la Directive (UE) 2015/1535 du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des règlementations techniques et des règles relatives aux services de la société de l'information (texte codifié).
11 S. Métille , « Introduction aux art. 269-281 CPP N 26 » in Y. Jeanneret /A. Kuhn /C. Perrier Depeursinge (ed.), *Commentaire romand CPP*, 2e ed., pp. 1733 ff., p. 1738, Bâle 2019.
12 Renvoi est fait à l'art. 3 de la Loi fédérale sur les télécommunications du 30 avril 1997 (LTC ; Recueil systématique du droit fédéral 784.10).
13 Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), Feuille fédérale 2013 2379, p. 2404. Critique à propos de cette définition très large, S. Métille, *op. cit.* (n. 11), pp. 1739.
14 ATF 143 IV 21, considérant 3.4 ; TF, 1B_142/2016, 16 novembre 2016, considérant 3.6. Pour une discussion relative au critère de la localisation des données vs le pouvoir de contrôle sur les données, voir J. Spoenle , *Cloud Computing and cybercrime investigations : Territoriality vs. the power of disposal ?*, Discussion Paper, Council of Europe, Economic Crime Division, Project on Cybercrime, 21 août 2010.
15 Code pénal suisse ; Recueil systématique du droit fédéral suisse 311.0.
16 Sur les liens avec la Décision d'enquête européenne, voir considérant 8 Règlement *e-Evidence*. À propos de l'(in)adéquation de la Décision d'enquête européenne concernant les preuves électroniques, voir S. Arasi, « The EIO Proposal and the Rules on Interception of Telecommunications » in S. Ruggeri (ed.), *Transnational Evidence and Multicultural Inquiries in Europe. Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Cham 2014, pp. 127 ff. ; C. Brière , « EU Criminal Procedural Law onto the Global Stage : The e-Evidence Proposals and Their Interaction with International Developments », *European Papers* 2021, pp. 493 ff., p. 499.
17 À propos de l'opportunité de procéder par le biais d'un formulaire standardisé, voir E. Casey et al., « The Evolution of Expressing and Exchanging Cyber-Investigation Information in a Standardized Form » in M. A. Biasiotto et al. (ed.), *Handling and Exchanging Electronic Evidence Across Europe*, Cham 2018, pp. 43 ss.
18 Voir toutefois les exceptions prévues à l'art. 8 par. 2 Règlement *e-Evidence*.
19 Ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication du 15 novembre 2017, Recueil systématique du droit fédéral suisse 780.117.
20 Pour une analyse détaillée du droit de la coopération internationale en matière de surveillance des télécommunications, voir U. Sieber/N. von zur Mühlen/T. Wahl, *Rechtshilfe zur Telekommunikationsüberwachung*, Berlin 2021 ; S. Tosza, « Cross-Border Gathering of Electronic Evidence : Mutual Legal Assistance, its Shortcomings and Remedies » in V. Franssen/D. Flore (ed.), *Société numérique et droit pénal. Belgique, France, Europe*, Bruxelles 2019, pp. 270 ff.
21 STE 185. Pour un manuel des bonnes pratiques en la matière, voir P. Verdelho, *The effectiveness of international co-operation against cybercrime : examples of good practices,* Report, Council of Europe, Economic Crime Division, Project on Cybercrime, 12 mars 2008. Voir aussi Comité de la Convention Cybercriminalité, du Conseil de l'Europe, Rapport d'évaluation : Les dispositions de la Convention de Budapest sur la criminalité concernant l'entraide, 2–3 décembre 2014, T-CY(2013)17rev.
22 Recueil systématique du droit fédéral suisse 351.1.
23 Voir L. Moreillon/S. Blank, « La surveillance policière et judiciaire des communications par Internet », *Medialex* 2004, pp. 81 ff. pp. 87. En revanche, l'entrée en vigueur pour la Suisse de la CCC a permis la transmission en temps réel de données informatiques relatives au trafic (art. 33 CCC ; la règle a été transposée en droit suisse à l'art. 18*b* EIMP). Les conditions sont toutefois restrictives et l'utilisation permise limitée.
24 À propos en particulier de l'inadéquation s'agissant des données stockées sur des *cloud*, voir L. Siry, « Cloudy days ahead : Cross-border evidence collection and its impact on the rights of EU citizens », *New Journal of European Criminal Law* 2019, pp. 227 ff., pp. 229 ff.
25 Pour une analyse détaillée des défis véhiculés par la portée internationale des moyens de preuve, voir J. D. Jackson/ S. J. Summers, *The Internationalisation of Criminal Evidence. Beyond the Common Law and Civil Law Traditions*, Cambridge 2012. Pour une proposition d'acte relatif à l'admissibilité des preuves, voir European Law Institute, Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings. Draft Legislative Proposal of the European Law Institute, 8 mai 2023 (à propos de cette proposition, voir L. Bachmaier, « Mutual Admissibility of Evidence and Electronic Evidence in the EU - A New Try for European Minimum Rules in Criminal Proceedings? », dans ce numéro).

# Electronic Evidence Collection in Cases of the European Public Prosecutor's Office

## Legal Framework, Procedures, and Specifics

Alexandru Frunza-Nicolescu*

**Electronic evidence (e-evidence) is necessary and relevant with regard to many cases of serious, organised, or cross-border crime. This is also true for cases investigated by the European Public Prosecutor's Office (EPPO). This article outlines the current legal framework, procedures, and mechanisms available to the EPPO for the collection of e-evidence in different case scenarios. It also takes into account the requirements for the protection of personal data, in particular arising in the transfer of operational data to authorities and private parties in third countries.**

### I. Introduction

The European Public Prosecutor's Office (EPPO) is the independent public prosecution office of the European Union responsible for investigating, prosecuting, and bringing to judgment crimes against the financial interests of the EU.[1] Like for any other national criminal justice authority, EPPO's success in investigating and prosecuting crime relies on the lawful, effective, and efficient collection of evidence.

The perpetrators of offences falling within EPPO's jurisdiction often make use of the Internet and information and communication technologies (ICTs) in the course of organising and committing their crimes, laundering the crime proceeds, or hiding the traces of their offences.

In general, computer data of any type or form can contain relevant traces of criminal activity. Thus, in order to prove that a crime has been committed, to identify the money laundering processes and the crime proceeds, and to bring the perpetrators to justice, the EPPO has to preserve, collect, assess, and make use of e-evidence in the investigations it carries out. Given the current architecture of the Internet and the significant number of Internet, social media, or communication services provided by companies located in foreign jurisdictions, e-evidence in many cases falls outside the territorial jurisdiction of the EPPO.[2]

Collecting cross-border e-evidence from foreign jurisdictions can be very challenging for any EU national judicial authority due to the scale and quantity of devices, users, and victims, the technical challenges like encryption or anonymisation, as well as territoriality and jurisdictional aspects.[3] Such collection requires knowledge and subsequent use of a variety of legal frameworks, procedures, cooperation networks, and technical arrangements. The structure, organisation, and legal framework of the EPPO – an EU indivisible body operating as a single office with a decentralised structure[4] – adds an additional layer of specific requirements to those already existing for traditional national criminal justice authorities.

In EPPO cases, e-evidence might be located, controlled, or stored in different jurisdictions, including: the jurisdiction of (1) the Member State of the handling[5] European Delegated Prosecutor (handling EDP); (2) the Member State of the assisting European Delegated Prosecutor (assisting EDP);[6] (3) a non-participating Member State;[7] (4) a party to the Council of Europe (CoE) Budapest Convention on Cybercrime,[8] including Denmark; (5) the EPPO non-participating Member State Ireland; and 6) any other third country not covered by scenarios one to five. In a seventh scenario, e-evidence might be controlled by foreign Internet and media service providers that can, in specific situations, share it directly with foreign criminal justice authorities on a voluntary basis, which is particularly true for providers based in the US. Each of these seven scenarios with their different rules, procedures, and mechanisms will be examined in the respective subsections of Section II. Section III. will be dedicated to the legality of transfers to third countries taking into account the relevant data protection rules in the EPPO Regulation before some concluding remarks in Section IV. The following analysis is based on the current legal framework and does not address the future legal framework on cross-border e-evidence collection following the entry into force of lined-up but not yet applicable EU and international in-

struments in the next few years, such as the EU e-evidence package[9] or the Second Additional Protocol to the Budapest Convention[10]. Neither will the article address in detail the issue of the competent jurisdiction over the computer data required by EPPO (i.e., questions regarding the determination of data location, storage place of data, location of the controller, location or nationality of data owner, etc.). The author rather assumes that the location of the data is established if the competent jurisdiction to be addressed by the EPPO in its request for computer data is to be considered.

## II. Case Scenarios

### 1. Scenario 1: e-evidence located within the territorial jurisdiction of the handling EDP

Computer data relevant for EPPO investigations might be located in the territory of the Member State participating in the EPPO of the handling EDP. In this case, the EDP will make use of the legal provisions, procedures, and technical arrangements available at national level, similar to any other criminal justice authority from his/her state. All 22 Member States participating in the EPPO are parties to the Budapest Convention on Cybercrime and have implemented the relevant provisions of the Convention in their criminal procedural law, thus insuring a certain harmonised level of procedural measures on computer data. These include: expedited preservation of stored computer data (Art. 16), production order (Art. 18), search and seizure of stored computer data (Art. 19), real-time collection of traffic data (Art. 20), and interception of content data (Art. 21). Based on the national provisions, the handling EDPs may order or request the issuing of the order (if judicial authorisation is required) for expedited preservation and/or production of computer data and ask the technical support to facilitate access to this data.

### 2. Scenario 2: e-evidence located within the territorial jurisdiction of an EPPO Member State other than the one of the handling EDP

If e-evidence is located in the territory of a Member State other than the one of the handling EDP, the latter can make use of the provisions of Art. 31 EPPO Regulation. This article represents a self-standing, *sui generis* legal basis for cross-border investigations of the EPPO.[11] The handling EDP sends an order for preservation/production of data to an assisting EDP from the Member State in question, who will then implement the measure there. If judicial authorisation is required under the legislation of the Member State where the data is located, the assisting EDP must obtain prior authorisation for the execution of the order from the competent court of his/her Member State.

### 3. Scenario 3: e-evidence located within the territorial jurisdiction of non-participating Member States other than Denmark and Ireland

To date, five EU Member States are not yet members of the EPPO. Three of them, i.e., Hungary, Sweden, and Poland, are bound by and have transposed in their national legislation Directive 2014/41 regarding the European Investigation Order in criminal matters (EIO Directive).[12] The collection of computer data which is located in the territory of one of these three non-participating Member States by the EPPO is governed by the provisions of the EIO Directive. In turn, the EIO is defined as a judicial decision issued or validated by a judicial authority in any one EU country for the gathering of evidence in criminal matters carried out in another EU country. Thus, in practice, the handling EDP will need to issue an EIO for the preservation/production of e-evidence on the basis of the national legal framework transposing the EIO in his/her country and send it for execution to the competent authority of the non-participating Member State. In this scenario, the EIO provides the EPPO with a simpler and faster alternative to the traditional mutual legal assistance instruments for requesting evidence, which are subject to strict deadlines and limited possibilities for refusal by the executing state.

### 4. Scenario 4: e-evidence located within the territorial jurisdiction of a Party to the Budapest Convention on Cybercrime (including non-participating Member State Denmark)

The Council of Europe Convention on Cybercrime (Budapest Convention) is a comprehensive and coherent international agreement on cybercrime and electronic evidence in criminal matters. It includes provisions to be implemented at national level, for both substantive and procedural law, and sets the rules for international cooperation for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form. To date, 68 countries are Parties to the Budapest Convention, including all EU Member States (except Ireland).

The Budapest Convention has high practical relevance for the criminal justice authorities of the Parties as it does not only concern computer-related crime, but any type of crime that requires the preservation/production of e-evidence. International cooperation in criminal matters under the Budapest Convention is regulated in Chapter III. For the preserva-

tion and collection of e-evidence, Section 2 of this Chapter (Arts. 29 to 34) is relevant, governing mutual legal assistance regarding provisional and investigative measures. The provisions include the following:

- Expedited preservation of stored computer data (Art. 29);
- Expedited disclosure of preserved traffic data (Art. 30);
- Mutual assistance regarding accessing of stored computer data (Art. 31);
- Trans-border access to stored computer data with consent or publicly available (Art. 32);
- Mutual assistance regarding real-time collection of traffic data (Art. 33);
- Mutual assistance regarding the interception of content data (Art. 34).

The Parties to the Budapest Convention can also make use of a 24/7 Network of contact points established under Art. 35. This network can facilitate the execution of preservation requests and production orders as well as provide assistance with regard to legal and technical information or locating suspects.

If data is located in a territory under the jurisdiction of a Party to the Budapest Convention, a criminal justice authority from another Party can apply the provisions of the Budapest Convention and request the preservation/collection of data directly, via the 24/7 Network, or via the authorities competent for international cooperation. While the EPPO is not a Party to the Budapest Convention and cannot make direct use of it, the handling EDP can make recourse to his/her powers as national prosecutor and request the data in accordance with the provisions of the Budapest Convention, under the conditions and limits set by Art. 104(5) EPPO Regulation. Accordingly, the handling EDP needs to "inform and where appropriate shall endeavour to obtain consent from the authorities of third countries that the evidence collected on that basis will be used by the EPPO for the purposes of [the EPPO] Regulation. In any case, the third country shall be duly informed that the final recipient of the reply to the request is the EPPO."

The handling EDP can also request the support of his/her country's 24/7 contact point or competent authority for sending and receiving mutual legal assistance (MLA) requests.[13] This can facilitate the process, as both the competent MLA authority and the 24/7 contact point have experience in working with the Budapest Convention and have established trustworthy relations with their counterparts from the other Parties to the Convention. In this context, Art. 28(1) EPPO Regulation enables the handling EDP "either to undertake the investigation measures and other measures on his/her own or instruct the competent authorities in his/her Member State." In a broad interpretation of this provision, the handling EDP can issue a preservation/production order and instruct the national 24/7 contact point or the competent national MLA authority to send the request to the competent foreign contact point/MLA authority of the third country.

However, the chances of success of requests made either on the basis of Art. 104(5) or Art. 28(1) EPPO Regulation will depend on the openness and willingness to cooperate on the part of the third country's national contact point/MLA authority or other competent authorities. For the future, concluding working arrangements with these third countries based on Art. 99(3) EPPO Regulation could be a feasible option to improve cooperation.

## 5. Scenario 5: e-evidence located or stored in the territory of Ireland

Ireland neither participates in the EPPO nor is it a Party to the Budapest Convention on Cybercrime; nor is it bound by the EIO Directive (see above). Nevertheless, given that a number of major US Internet and social media providers are headquartered in Ireland, there is an important need to cooperate with the Irish authorities for securing and collecting e-evidence. Currently, the only possible option for any national criminal justice authority in the EU to collect e-evidence from the Irish jurisdiction is the use of traditional methods of international cooperation, i.e. using the MLA channels of the two applicable EU and CoE mechanisms: (1) Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union[14] and its Protocol, and (2) the European Convention on Mutual Assistance in Criminal Matters[15] and its two additional Protocols.

Despite the fact that all Member States participating in the EPPO have notified it as a competent authority for the application of the 2000 EU MLA Convention, Ireland has refused in practice to recognise these notifications and has been consistently rejecting the EPPO's requests for judicial cooperation.[16]

However, there is hope for the future. Ireland has a flexible opt-out option from EU legislation applicable in the area of freedom, security, and justice that allows the country to opt in or out of legislative initiatives on a case-by-case basis. As a result, Ireland has notified its wish to take part in the adoption and application of the EU's recent e-Evidence Regulation (Regulation (EU) 2023/1543)[17] due to enter into force in 2026. After the entry into force of this Regulation, EU criminal justice authorities will be able to issue

and send preservation and production orders directly to service providers established in Ireland, with the latter having the obligation to provide the requested data under the conditions stipulated by the new EU legal framework on e-evidence.

### 6. Scenario 6: e-evidence located in the territory of a third country not covered by scenarios 1 to 5

For the collection of e-evidence from any jurisdiction not covered by the previous five scenarios, the EPPO needs to make use of the traditional channels of international cooperation in criminal matters, applicable to the collection of "classic" evidence. Cooperation with these jurisdictions can be based on two different scenarios: First, the EU is party to an international instrument on judicial cooperation and has declared the EPPO's competence for that particular instrument. Second, a Member State participating in the EPPO is party to an international agreement in criminal matters and it has notified EPPO as the competent authority for that specific instrument.

The EU has acceded to the UN Conventions against Transnational Organized Crime (UNTOC) and against Corruption (UNCAC). Accordingly, it has updated its declarations of competence for these UN Conventions and notified the EPPO as competent authority. However, the notification of the EPPO as competent authority for the purpose of these multilateral conventions is subject to the acceptance of the other Parties. All Member States participating in the EPPO have notified the CoE of the update to the list of competent authorities for the purpose of the 1959 MLA Convention and its additional Protocols and included the EPPO.

UNTOC, UNCAC, and the 1959 CoE MLA Convention are complemented by other bilateral or multilateral agreements on international cooperation in criminal matters signed by the Member States participating in the EPPO. Also here, the respective Member States participating in the EPPO must notify the EPPO as competent authority to their counterparts.

As regards cooperation with the United Kingdom, the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community and the United Kingdom of Great Britain and Northern Ireland (TCA) is applicable.[18] The EU has already notified the EPPO as competent authority for the application of the relevant MLA provisions of the TCA.

Similar to the cooperation with the Parties to the Budapest Convention, the handling EDP can also require e-evidence from other third countries by making use of the provisions of Art. 104(5) or Art. 28(1) EPPO Regulation. Likewise, the result of such requests will depend on the openness and willingness to cooperate on the part of the third country's competent authorities (see above).

### 7. Scenario 7: cooperation with US-based Internet and media service providers – voluntary disclosure

Relevant computer data is often stored and controlled by Internet and media service providers based in the United States (US ISPs), with the servers located in the US. The collection of this data through traditional MLA instruments, including the 2003 MLA Agreement between the EU and the USA[19], can be time-consuming and inefficient, with response times varying from six months to two years.[20] The EPPO has not yet been notified as competent authority for said MLA Agreement but has signed a memorandum of understanding and working arrangement with the US Department of Justice (DOJ) and the Department of Homeland Security (DHS),[21] in which the US side emphasised its intention to cooperate with the EPPO in the collection of evidence in EPPO cases "consistent with applicable legal frameworks."[22] The DOJ has asserted that it will "provide mutual legal assistance in response to a request made on behalf of a European Delegated Prosecutor handling the matter and transmitted between the appropriate authority of the EU Member State in which the investigation or prosecution is being carried out and the U.S. Central Authority for mutual legal assistance."[23]

However, several major US ISPs disclose data to foreign authorities on a voluntary basis – an approach which is also backed by US legislation. This is a pragmatic and lawful option to overcome some of the difficulties in swiftly obtaining e-evidence from the US. Google, Meta, Amazon, Apple, X, and others regularly disclose subscriber information or traffic data, and in some very limited cases, content data, to foreign criminal justice authorities, without requiring an MLA request sent via the competent US authorities. They also accept preservation requests directly sent to them by foreign authorities and have established dedicated teams to handle law enforcement and judicial requests for data. Transparency reports issued by said providers show that computer data is shared with foreign authorities in a significant number of cases.[24]

Voluntary disclosure of data by the US ISPs is problematic for the lack of predictability of the procedure and the discretionary power in the hands of the providers. Nevertheless, voluntary disclosure remains an option that can bring results and can facilitate the start and continuation of an in-

vestigation, at least until 2026 when the new EU e-evidence legislation will bring about important modifications.

A useful tool for contacting the specific US ISPs and for requesting the preservation of computer data, subscriber information, and traffic data is the "Practical Guide for Requesting Electronic Evidence Across Borders"[25] developed by UNODC jointly with several other international organisations and EU agencies. This guide is regularly updated and provides relevant practical information on the procedure, rules, and paths to be used by criminal justice authorities. While it is restricted to criminal justice practitioners, it can be accessed by practitioners working in the EU via the Europol Platform for Experts (EPE) and by all other criminal justice practitioners on the UNODC SHERLOC platform.

## III. Data Protection Issues

The processing of operational personal data by the EPPO is governed by Arts 47 to 89 EPPO Regulation. Whenever the EPPO seeks to obtain electronic evidence from a competent authority or a private entity of a third country, including the non-EU parties to the Budapest Convention, it will, in most cases, provide some operational personal data to that authority/private party. For example, in order to request data preservation for a Gmail account, some operational personal data with regard to that email account needs to be disclosed. In addition, most of the third countries' authorities and private parties will request information on the crime, suspects, place, date etc. in order to reply to EPPO's request for data. For all these situations, the provisions of Art. 80 EPPO Regulation regarding the general principles for transfers of operational personal data by the EPPO are applicable. Similar to other EU legislation on the protection of personal data in criminal matters and international cooperation in criminal matters (e.g., the Law Enforcement Data Protection Directive[26], the Europol Regulation[27], and the Eurojust Regulation[28]), the EPPO Regulation provides for a limited number of cases in which the EPPO is allowed to transfer operational personal data to authorities or private parties outside the EU.

A transfer pursuant to Art. 81 EPPO Regulation is currently not an option for the EPPO as no adequacy decision has been issued by the European Commission on the basis of Art. 36 Directive (EU) 2016/680. As far as cooperation with the United Kingdom is concerned, the EPPO can rely on Art. 82(1) lit. a) EPPO Regulation because the TCA (as a legally binding instrument) includes appropriate safeguards with regard to the protection of operational personal data. In other cases, the EPPO can make recourse to the provisions of Art. 82(1) lit. b) or Art. 83 EPPO Regulation. According to Art. 82(1) lit. b) EPPO Regulation, transfers to third countries are possible when the EPPO has assessed all the circumstances surrounding the transfer of operational personal data and concluded that appropriate safeguards are in place with regard to the protection of personal data in that third country. Art. 83 EPPO Regulation stipulates derogatory situations in which transfer is specifically possible.[29] In the case of a possible transfer of operational personal data both on the basis of Art. 82(1) lit b) and Art. 83 EPPO Regulation, and subsequent transfer of operational personal data, the handling EDP needs to carry out an assessment and fill in a report/note justifying the measure prior to sending a request for e-evidence. This report/note must be registered in EPPO's Case Management System (CMS).

The assessment made by the handling EDP on whether the third country has appropriate safeguards with regard to the protection of personal data may take into consideration, *inter alia*, the current working arrangements concluded by the EPPO on the basis of Art. 99 EPPO Regulation with authorities of the respective third country. While Art. 99(3) EPPO Regulation explicitly stipulates that the working arrangements "may neither form the basis for allowing the exchange of personal data nor have legally binding effects on the Union or its Member States," the EDP is free to consider the data protection provisions in the working arrangement as one (but not the only one) element supporting his/her assessment of the existence of appropriate safeguards.

In future, Art. 82(1) lit a) EPPO Regulation (transfers on the basis of appropriate safeguards in a legally binding instrument) will gain importance when the Second Additional Protocol to the Cybercrime Convention[30] and a modernised Council of Europe Data Protection Convention ("Convention 108+")[31] enter into force and are ratified by a number of third countries.

## IV. Conclusion

Given the increasing number of EPPO investigations, in which computer data are required to prove the commission of a criminal offence and to identify the perpetrators and the crime proceeds, the EPPO has to apply the legal frameworks, rules, procedures, and networks at its disposal. Otherwise, the EPPO could not efficiently collect such computer data and transform them into evidence accepted at

trial. The applicable instruments for EPPO's handling EDPs vary depending on where the data are located. As has been shown in this article, sometimes complementary instruments apply, and sometimes the competent EDP must find pragmatic ways to obtain the best results.

In most cases, cross-border requests for e-evidence involve the (initial) transfer of operational personal data by the EPPO to authorities or private parties outside the European Union. Thus, the protection of personal data must be taken into thorough consideration, and the EDP must undertake to justify the transfer of personal data to third countries in line with the data protection rules in the EPPO Regulation in several ways.

Legal developments at the EU and international levels will unlock further possibilities for the EPPO to collect e-evidence in future. However, respecting the individual rights of data subjects must remain paramount even under these new set-ups.

**Alexandru Frunza-Nicolescu**
Senior Legal Assistant, European Public Prosecutor's Office (EPPO)

∗ The views expressed in this article are exclusively those of the author and cannot be attributed to the institution that employs him.

1 Cf. <https://www.eppo.europa.eu/en/mission-and-tasks>. All links in this article were last accessed on 29 September 2023.

2 Commission Staff Working Document, Impact Assessment – Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD(2018) 118 final, p. 14.

3 Cybercrime Convention Committee (T-CY), *Criminal justice access to data in the cloud: challenges - Discussion paper*, 26 May 2015, <https://rm.coe.int/1680304b59>.

4 Art. 8 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), *O.J.* L 283, 31.10.2017, 1. Hereinafter: EPPO Regulation.

5 Art. 2(5) EPPO Regulation: "'handling European Delegated Prosecutor' means a European Delegated Prosecutor responsible for the investigations and prosecutions, which he/she has initiated, which have been allocated to him/her or which he/she has taken over using the right of evocation according to Article 27."

6 Art.2(6) EPPO Regulation: – "'assisting European Delegated Prosecutor' means a European Delegated Prosecutor located in a Member State, other than the Member State of the handling European Delegated Prosecutor, where an investigation or other measure assigned to him/her is to be carried out."

7 As of September 2023, these are: Denmark, Hungary, Ireland, Poland, and Sweden.

8 CETS No. 185, available at: <https://rm.coe.int/1680081561>.

9 Cf. <https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en>.

10 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224>.

11 Section 1, Article 1 of the Decision of the College of the European Public Prosecutor's Office of 26 January 2022 adopting Guidelines on the Application Of Article 31 Of Regulation (EU) 2017 /1939, available at: <https://www.eppo.europa.eu/sites/default/files/2022-02/2022.006_Decision_adopting_Guidelines_on_the_application_of_article_31_of_the_EPPO_Regulation.pdf>.

12 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *O.J.* L 130, 1.5.2014, 1.

13 Art. 27 para. 2 lit.a) Budapest Convention on Cybercrime: Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their *transmission to the authorities competent for their execution* (emphasis by author).

14 *O.J.* C 197, 12.7.2000, 3.

15 CETS No. 030.

16 Cf. <https://www.eppo.europa.eu/en/news/european-chief-prosecutor-addresses-letter-commission-irelands-refusal-cooperate-eppo>.

17 Regulation (EU) 2023/1543) of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *O.J.* L 191, 28.7.2023, 118.

18 *O.J.* L 149, 30.4.2021, 10.

19 Agreement on mutual legal assistance between the European Union and the United States of America, *O.J.* L 181, 19.7.2003, 34.

20 T-CY assessment report: *The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, p. 123, available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>.

21 Memorandum of Understanding and Working Arrangement on Cooperation between the European Public Prosecutor's Office, on the one side, and the United States Department of Justice and Department of Homeland Security, on the other side, available at: <https://www.eppo.europa.eu/sites/default/files/2022-07/WA%20EPPO-US-signed-EPPO.pdf>.

22 Memorandum of Understanding and Working Arrangement, *op. cit.* (n. 21), Section 3.

23 *Idem* 13.

24 T-CY, *Criminal justice access to data in the cloud: Cooperation with "foreign" service providers* – Background paper, 3 May 2016,

available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d>.
25 Cf. <https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html>.
26 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA., *O.J.* L 119, 4.5.2016, 89.
27 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA., *O.J.* L 283, 31.10.2017, 1.
28 Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA., *O.J.* L 295, 21.11.2018, 138.
29 (a) in order to protect the vital interests of the data subject or another person; (b) to safeguard legitimate interests of the data subject; (c) for the prevention of an immediate and serious threat to public security of a Member State of the European Union or a third country; or (d) in individual cases for the performance of the tasks of the EPPO, unless the EPPO determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer.
30 Cf. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224>.
31 Cf. <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0>.

# Gathering Electronic Evidence for Administrative Investigations

## Exploring an Under-the-Radar Area

Stanisław Tosza

**The intense debate over the past few years on access to data for criminal investigations has led to the adoption of the E-evidence package. Yet, electronic evidence is no less crucial for punitive administrative proceedings. One administrative investigation authority that could benefit from more extensive access to electronic evidence is OLAF, which, at this point, does not seem to have the power to request data from service providers. Such powers could be essential, however, for the detection and investigation of fraud or corruption. This article argues the need for a general and thorough reflection on access to electronic evidence from Internet Service Providers (ISPs) in administrative punitive proceedings. It also discusses the transfer of this type of evidence between administrative and criminal proceedings (in both directions) in order to more specifically justify an extension of OLAF's powers to be able to request such evidence.**

### I. Introduction

With the ever-increasing digitalisation of almost every aspect of human activities, any type of infringement – be it criminal or administrative – leaves digital traces, which may become crucial as evidence in punitive proceedings. Yet, access to electronic evidence is far from straightforward, as it is often in the hands of foreign service providers. Outdated rules of territoriality thus hamper law enforcement efforts, because instruments of international cooperation, such as mutual legal assistance, must be used, which complicate the procedure and render it disproportionately lengthy.[1] This is linked with the fact that often the data has to be obtained from US service providers given their market share. However, US law in principle prohibits the transfer of content data to foreign law enforcement without a decision of a US judge.[2] Numerous other factors of a legal and practical nature add complexity to the problem, such as encryption,[3] rules on admissibility of evidence,[4] and limitations of enforcement capacity,[5] to name just a few.

Three major initiatives are intended to remedy this situation, although it is too early to assess their impact. First, the EU has just adopted the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, which aims at addressing the above-mentioned difficulties.[6] Most importantly, it will allow law enforcement authorities in one Member State to compel service provid-

ers in another Member State to produce data without engaging the authorities of the latter. Second, the EU is negotiating an agreement on e-evidence with the USA, which would broaden the possibilities of US service providers to transmit data to foreign law enforcement authorities without the decision of a US judge.[7] Third, the recently adopted Second Protocol to the Cybercrime Convention also provides for possibilities to directly request data cross-border from digital companies, even if this would apply only to limited types of data.[8]

All these initiatives open the door to direct cross-border cooperation between law enforcement authorities and service providers, which is not without controversy and creates different legal problems. Intense debate during the lengthy process of negotiating the E-evidence Regulation (and its accompanying Directive) concerned such issues as: its legal basis,[9] the future relationship between the European Production Order and the European Investigation Order,[10] the role of EU data protection law,[11] and the future relationship with the US legal framework.[12] The adoption of the E-evidence package will not end the debate, rather the contrary. One of the most important questions is how service providers can be gatekeepers and protectors of fundamental rights while retaining a private entity nature.[13]

Administrative law enforcement has been notably absent from these debates and initiatives. The European E-evidence Regulation will solely apply to criminal proceedings.[14] Also, the Second Protocol to the Cybercrime Convention is limited to criminal investigations only.[15] Yet, electronic evidence is no less crucial for punitive administrative proceedings. Although access to electronic evidence will arguably not be as broad as that for criminal investigations, due to privacy limitation concerns, it will be increasingly more difficult to miss the golden opportunity that access to evidence through service providers offers for effective investigations. Already non-content data offers insights that may be essential for providing proof of misconduct.[16]

An administrative investigation authority that could benefit from more extensive access to electronic evidence is the European Anti-Fraud Office (OLAF), which so far has no specific provisions on cooperation with Internet Service Providers (hereinafter: ISPs). The need to access new types of evidence is well exemplified by the recently added possibility for OLAF to request bank account information.[17] However, we may find possibilities to access electronic evidence in other administrative proceedings, e.g., in financial supervision and the Market Abuse Regulation.

This article aims to sketch out the problem of gathering of electronic evidence in the context of administrative punitive enforcement and the need for research in this area. A particular focus will be placed on OLAF, its need for electronic evidence, and the lack of legal basis to request data from service providers. The article will also briefly present a recently launched research initiative to further explore this issue.

## II. Need for Electronic Evidence

The distinctiveness of electronic evidence – contrary to more traditional sources of evidence – is that it can be obtained through a third party: the service provider. This feature is unique: even if access to written letters was possible as a criminal procedural measure, the traditional postal service neither had regular access to the content of the letters they delivered nor did they regularly gather metadata on these letters. In contrast, email service providers do both. Starting from the possibility to acquire data from telecommunication providers,[18] access to data from different kinds of ISPs has become crucial for successful investigations in recent years.

Data in possession of ISPs may be a treasure trove for enforcement authorities. The nature of cyberspace clashes with the limitations of enforcement, however, which hinder access to the data. While data can flow unhindered, at least in principle, law enforcement remains confined to national borders as prescribed in the seminal Lotus judgment.[19] In its conventional reading, the principle of territoriality mandates that if the data being sought is stored outside of the country of investigation, then instruments of cross-border cooperation need to be used, which renders access much more time-consuming, costly, and cumbersome.[20] This duality – attractiveness of electronic evidence gathered from third parties and inaptness of principles governing enforcement in cyberspace – characterises this field and has triggered a number of legislative and jurisprudential initiatives.

Over the past several years, the debate over access to electronic evidence gained prominence as regards access to data for criminal investigations. The laws of criminal procedure allowed the authorities to access this data, while providing the framework for protecting suspects' procedural safeguards. However, if the service provider was located in another country or the data was stored abroad, law enforcement was supposed to resort to instruments of cross-border cooperation: the European Investigation Order (EIO) within the EU's area of freedom, security and justice and mutual legal assistance (MLA) outside this area, in particular regarding content data from US companies.[21]

The necessary paperwork for MLA and the length of the procedure, compulsory even in purely local cases, garnered frustration on the part of law enforcement, leading to the use of voluntary cooperation with ISPs and to a reinterpretation of the principle of territoriality.[22] As to the latter, Belgium for instance decided to treat foreign providers actively targeting Belgian clients as if they were national providers. In two famous cases concerning Yahoo and Skype, these companies found themselves obliged to produce data according to a Belgian order, although the law of the place where they were headquartered (USA and Luxembourg, respectively) prohibited them from doing so.[23]

The ensuing discussion resulted in the adoption of the EU's E-evidence package (composed of a Regulation and a Directive), which offers a much faster way to gather electronic evidence in criminal proceedings. While the Regulation (hereinafter: EPOR) creates the new instruments of the European Production and Preservation Orders, the Directive is meant to ensure that there is at least one potential addressee for the newly created orders per each service provider entering the scope of the EPOR. The main premise of the Regulation is that competent authorities are entitled to issue binding requests to service providers offering services within the EU regardless of their place of establishment or the physical location of the data. Law enforcement authorities in one Member State will now be allowed to issue orders that are directly transmitted to private actors in a different Member State and which have to be executed without any involvement of the authorities of that Member State (with a number of limited exceptions).[24]

## III. Electronic Evidence in Administrative (Punitive) Investigations

It is a truism that the nature of administrative proceedings is different from that of criminal proceedings. Administrative decisions do not carry the stigma and moral reproach of criminal law punishments, and instruments of administrative law are less intrusive overall. They also serve different objectives and are not focused on prevention, retribution, or reparation in the same way as criminal enforcement; most of all, they are meant to ensure compliance with the regulatory legal framework.[25] However, punitive administrative proceedings may be sufficiently punitive to justify being treated as a "criminal charge" according to the *Engel* jurisprudence.[26]

In order to be effective, administrative authorities need to have efficient and modern tools at their disposal to gather evidence for these proceedings, with electronic evidence gathered from ISPs wielding increasing influence over enforcement in recent years. There are four ways in which administrative authorities may acquire this type of evidence from the service providers:

First, there may be a concrete legal basis allowing them to make such requests. For example, the Market Abuse Regulation (596/2014) provides that, under certain circumstances, competent authorities shall have the power to request existing data traffic records held by a telecommunications operator (Art. 23 (2) (h)). Particularly at the national level, however, such access may be controversial. For instance, the French legal framework regarding access to telecommunication data by administrative authorities has evolved dramatically during the last few years. Even though the case law of the European Court of Justice has been subject to criticism in France, the French Constitutional Council struck down several laws that did not take into consideration privacy and data protection, following the case law of the ECJ.[27] One interesting feature of the current legal framework is the creation of a new authority in charge of allowing these measures (*le contrôleur des demandes de données de connexion*).[28]

Secondly, data may be potentially requested from service providers by means of a more general legal basis concerning a request for information.[29] For instance, the European Central Bank may request data based on Art. 10 (1) (f) of SSM Regulation No 1024/2013. The Commission's Directorate General Competition may request information from third parties based on Art. 18 of Regulation 1/2003, which does not preclude using it to request information from ISPs. Competent national authorities may proceed similarly.

Thirdly, administrative enforcement authorities may simply request data from service providers on a voluntary basis. These requests are not binding for ISPs. This practice developed in criminal investigations due to the shortcomings of compelling ways of requesting data described above. It relies on the general willingness of ISPs to cooperate with law enforcement and allows the authorities to circumvent the problem of territoriality and the necessity of using cooperation instruments. However, such practice results in that the ISPs *de facto* take the responsibility to assess the legality and proportionality of the requests becoming guardians of the fundamental rights of their users instead of public authorities. Contrary to public authorities, however, the ISPs will perform such assessment in accordance with their business interest.[30]

Fourthly, electronic evidence may be transferred from other proceedings, be they administrative or criminal, if the law

so permits. As established by the ECJ in *WebMindLicences*, in fact, EU law does not preclude administrative procedures from using evidence obtained in the context of a parallel criminal procedure that is still ongoing, provided that the rights guaranteed by EU law are observed.[31]

## IV. OLAF and Gathering of Electronic Evidence

OLAF, at this point, does not appear to have the power to request data from service providers, which might be essential for the detection and investigation of fraud or corruption. OLAF needs to extend its powers in a way that reflects modern realities, as demonstrated by the addition of the possibility for OLAF to request bank account information.[32] In order to protect EU financial interests, in particular to combat fraud, corruption, and any other illegal activities affecting them, electronic evidence will become increasingly relevant.

OLAF has also a less advantageous position in this respect than the European Public Prosecutor's Office (EPPO). European Delegated Prosecutors (EDPs) will have different possibilities to request and receive data from service providers, even if the legal framework as regards issuing European Production Orders by EDPs presents some interpretative problems,[33] and the silence of the EPOR in this respect is not helpful.[34] In any case, national measures of criminal procedure may certainly be used to acquire electronic evidence and there will be a possibility to issue orders to non-participating Member States (including Ireland).

It is therefore necessary to provide a general and thorough reflection on access to electronic evidence from ISPs in administrative punitive proceedings and on the transfer of this type of evidence in administrative and criminal proceedings (in both directions), in order to more specifically justify the possibility for OLAF to extend its powers to be able to request such evidence. It is necessary to examine whether OLAF should have the power to request the ISPs to produce data and, if so, to what extent (which data, in which circumstances, etc). Despite entering into the remit of EPPO, OLAF remains crucial for protecting the EU's financial interests in several contexts: internal investigations,[35] countries that do not participate in the EPPO,[36] investigations involving third countries, [37] cases in which the EPPO decided not to open investigation,[38] and where OLAF's support has been requested.[39] In order to better protect the EU budget, OLAF needs to permanently increase the efficiency of its investigations. The newly acquired power to request bank statements is a good example of how it is venturing into waters traditionally associated with criminal investigations. Information held by ISPs is surely of great interest in OLAF investigations, for example enabling OLAF to identify perpetrators/accomplices in fraud and/or corruption investigations, which are typically characterised by hidden arrangements, or to demonstrate the organised nature of criminal groups targeting the EU budget (e.g., the same organisations are behind different email addresses used in custom fraud). At the same time, the gathering of data has to be done in ways that ensure protection of the right to privacy and safeguard the right to data protection.

Furthermore, and given OLAF's role, it is necessary to establish the conditions under which evidence gathered in this way can be transferred to a criminal investigation (e.g., to the EPPO) or how it can be transferred from a criminal investigation to an administrative one. Transfer of evidence from OLAF to criminal investigations is currently governed by Art. 11(2) of the OLAF Regulation, according to which OLAF's final reports, together with all supporting evidence annexed to them, shall constitute admissible evidence in administrative or judicial proceedings of a criminal or non-criminal nature, before national courts or before the CJEU, according to the type of irregularity or fraud identified.[40]

OLAF must strive to make its investigations consistently more efficient and effective,[41] adapting to operating in a challenging, fast-paced environment. The nature of irregularities and fraud has changed significantly in recent years and keeps shifting in keeping with an exceedingly more digitised world. The trans-border dimension of fraud as well as rapid technical advances in the European Union and worldwide demand a response at the EU level.

The Internet of Things is ever accelerating and permeates all aspects of life, including the life of perpetrators of fraud and irregularities. Too often, irregularities and fraud are hidden behind perfect paperwork. Artificial circumstances created to gain EU funding by collusion and under-evaluation or other wrongdoing[42] can only be detected and revealed through information held by ISPs. Cases that rely on the availability of social media evidence[43] are just one example, as fraudsters seem to increasingly (ab)use the deep or dark web for illicit financial transactions in cryptocurrencies. Ongoing studies on how blockchain technology can be used to procure EU funding and for public procurement only accentuate the need to cover this ground.[44] As a European centre for knowledge, intelligence, and competence in anti-fraud matters at the EU level, OLAF should be able to (and certainly cannot afford not to) address this development, also in its investigative activities.

One of the questions that remains to be answered is how to design OLAF's competence to request electronic evidence

from ISPs. Should it be a system analogous to OLAF's access to bank accounts?[45] Another question is to what extent access to information by ISPs complies with,[46] or should be accompanied by, supplementary judicial control? Within OLAF's administrative investigative remit, such power could be equated with that of national investigators and, relying on conditions of national law, could possibly include assistance by national anti-fraud coordination services[47] and/or judicial review.

In cases in which OLAF assists a criminal investigation by the EPPO,[48] the Office would act, within its mandate, under the direction of the handling EDP. The latter would then be responsible for assessing the legality and regularity of his/her own request under EU and national law.

Access to data by OLAF should also respect principles of proportionality, necessity, and data protection. All OLAF's investigations need to be conducted objectively and impartially, in accordance with the principle of the presumption of innocence, and with respect to procedural guarantees.[49] The current legal framework, including internal guidelines, already provides a structure by which to control compliance with procedural guarantees and data protection rules. A request for access to information held by ISPs would arguably warrant at least the following:

- Assessment of the necessity and proportionality of the request;
- Authorisation by OLAF's Director-General, possibly after internal review;
- An independent monitoring and complaints mechanism which is handled by the Controller of Procedural Guarantees50 and OLAF's Supervisory Committee.51

## V. Need for Further Research

Although access to electronic evidence for the purpose of criminal investigation has been subject to extensive research efforts,[52] there has been no systematic research to date in the field of administrative investigations as to the legal possibilities for requesting electronic evidence from ISPs. There is no knowledge about the practice itself, in particular as regards the use of a general legal basis or voluntary cooperation. These matters are the subject of the recently started project "Gathering electronic evidence for administrative investigations – comparative study of law and practice" (ELEVADMIN) hosted by the University of Luxembourg and financed by OLAF.[53]

Its objective is to examine the already existing legal framework at the national (in nine selected Member States) and EU levels and especially to understand the practice of gathering electronic evidence from ISPs for administrative investigations. The study will cover the gathering of electronic evidence in administrative punitive proceedings in the following areas:

- Protection of the EU's financial interests (PIF);
- Customs enforcement;
- Tax enforcement as regards VAT;
- Punitive enforcement in the area of banking and financial markets;
- Competition law enforcement.

The information gathered will be the subject of a comprehensive comparative analysis and in this way provide an extensive examination of the law and practice of gathering electronic evidence from ISPs in the context of punitive administrative enforcement. This analysis will also enable the formulation of policy goals for OLAF and for its potential extension of competencies.

## VI. Conclusions

Despite the recent adoption of the E-evidence package, the electronic evidence question will remain a problematic issue in the years to come. Over the next three years, which are intended to have the necessary legislation for national rules to the EPOR adapted, numerous questions have to be answered, and the technical capacity for exchange of data must be provided.[54] The outcome of the negotiations with the USA on the agreement to allow unmediated cross-border exchange of electronic evidence between law enforcement and service providers will have a significant impact on how this evidence is gathered and will be crucial for the efficiency of the EPOR. Lastly, it remains to be seen how many countries will sign and ratify the Second Protocol to the Cybercrime Convention and what impact it will have on ensuing national legislation.

The increasing transfer of human activity to cyberspace, which will exacerbated even more by the entry into adult life of new generations of digital natives, will continue to put pressure on the rules of enforcement to adapt to this new reality. An area in which access to electronic evidence remains largely unaddressed is administrative punitive enforcement. In order to increase its efficiency and keep pace with technological developments, administrative investigations, such as the ones undertaken by OLAF, will have to be equipped with the possibility to acquire electronic evidence through cooperation with Internet service providers. A simple "transplant" of rules developed in the field of criminal investigation is not a viable possibility,

given the nature and objectives of administrative law and the potential intrusiveness of gathering of personal data. Thus, a thorough reflection is needed on the needs and limits of gathering electronic evidence for administrative investigations. Such a reflection could be part of a broader discussion on the role of technology in enforcement and on challenges created by constant technological developments, including the gathering and examining of evidence by means of Internet of Things and Artificial Intelligence. OLAF and the EPPO should not lag behind in such developments, and the interaction between the two enforcement bodies in electronic evidence gathering will be of key importance in the field of the protection of the EU's financial interests.

* The article was prepared within the framework of the project "Gathering electronic evidence for administrative investigations. Comparative study of law and practice (ELEVADMIN)", co-financed by the EU/Union Anti-Fraud Programme (EUAF), Project 101101776 — 2022-LU-ELEVADMIN. The views and opinions expressed are those of the author only and do not necessarily reflect those of the European Union or the European Commission.

**Prof. Dr. Stanisław Tosza**
Associate Professor in Compliance and Law Enforcement, University of Luxembourg

1 D. J. B. Svantesson, *Solving the Internet Jurisdiction Puzzle*, 2017; J. Daskal, "The Un-Territoriality of Data", (2015) *The Yale Law Journal*, 326; S. Tosza, "All evidence is equal, but electronic evidence is more equal than any other. The relationship between the European Investigation Order and the European Production Order", (2020) *New Journal of European Criminal Law*, 161.

2 J. Daskal, "Unpacking the CLOUD Act", (2018) *eucrim*, 220.

3 O. S. Kerr and B. Schneier, "Encryption Workarounds", (2018) *Georgetown Law Journal*, 989.

4 See European Law Institute, "ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings", 2023, available at: <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf>. For this proposal, see the article by L. Bachmaier in this issue.

5 S. Tosza, "Cross-Border Gathering of Electronic Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies", in: D. Flore and V. Franssen (eds.), *Société numérique et droit penal*, 2019, p. 269.

6 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *O.J.* L 191, 28.7.2023, 118–180; Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *O.J.* L 191, 28.7.2023, 181–190.

7 Directorate-General for Justice and Consumers, Statement of 2 March 2023, "EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations", <https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en>, accessed 2 November 2023.

8 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

9 V. Mitsilegas, "The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence," (2018) *Maastricht Journal of European and Comparative Law*, 263; K. Ligeti and G. Robinson, "Transnational Enforcement of Production Orders for Electronic Evidence. Beyond Mutual Recognition?", in: R. Kert and A. Lehner (eds), *Vielfalt des Strafrechts im internationalen Kontext: Festschrift für Frank Höpfel zum 65. Geburtstag*, 2018, 625–644.

10 S. Tosza, (2020) *New Journal of European Criminal Law, op. cit.* (n. 1).

11 F. Fabbrini and E. Celeste and J. Quinn (eds.), *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty*, 2021.

12 J. Daskal, (2018) *eucrim, op. cit.* (n. 2), 220.

13 S. Tosza, "Internet service providers as law enforcers and adjudicators. A public role of private actors", (2021) *Computer Law & Security Review,* 1–17.

14 The future agreement with the USA will also most probably be limited to criminal investigations only, cf. U.S. Department of Justice, White Paper, April 2019, <https://www.justice.gov/opa/press-release/file/1153446/download> accessed 2 November 2023.

15 Art. 2 of the Second Additional Protocol to the Convention on Cybercrime.

16 B. Schneier, *Data and Goliath*, 2015, p. 26.

17 Art. 7 (3a) Regulation 883/2013 as amended by Regulation 2020/2223 (OLAF Regulation). For an overview of the 2020 reform of the OLAF Regulation see M. Bellacosa and M. De Bellis, "The protection of the EU financial interests between administrative and criminal tools: OLAF and EPPO", (2023) *Common Market Law Review*, 15–50.

18 See for instance R. Kert and A. Lehner, "Austria"; in: K. Ligeti, *Toward a Prosecutor for the European Union. Volume 1*, 2013, p. 29; J. Tricot, "France", in: K. Ligeti, *ibid*, p. 238–240; T. Weigend, "Germany" in: K. Ligeti, *ibid*, 278–279; see also C. Larsson, "Telecom Companies as Crime Investigators", (2004) *Scandinavian studies in law*, 421–450; Council Resolution of 17 January 1995 on the lawful interception of telecommunications, *O.J.* C 329, 4.11.1996.

19 Permanent Court of International Justice on 7 September 1927 in the case of SS Lotus, Publications of the Permanent Court of International Justice, Series A.-No. 70, 18–19.

20 U. Sieber and C. Neubert, "Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty", (2017) 20th Max Planck Yearbook of United Nations Law Online, 239.

21 J. Daskal, (2018) *eucrim, op. cit.* (n. 2), 222.

22 K. Ligeti and G. Robinson, "Sword, Shield and Cloud: Toward a European System of Public–Private Orders for Electronic Evidence in Criminal Matters?" in: V. Mitsilegas and N. Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives*, 2021, p. 27; S. Tosza, (2020) *New Journal of European Criminal Law*, *op. cit.* (n. 1).
23 V. Franssen, "The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?", (2017) *European Data Protection Law Review*, 534, 538 ff.
24 See S. Tosza, "European Union, The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?", (2023) *European Data Protection Law Review*, 163.
25 C. Harlow and G. Cananea and P. Leino, "Introduction: European administrative law – a thematic approach" in: C. Harlow (ed.), *Research handbook on EU administrative law*, 2017, p. 2.
26 ECtHR, 8 June 1976, *Engel and Others v. The Netherlands*, Appl nos 5100/71; 5101/71; 5102/71; 5354/72; 5370/72.
27 Conseil Constitutionnel n° 2021-976/977 QPC du 25 février 2022.
28 Art. L. 621-10-2 Code monétaire et financier.
29 M. Luchtman and J. Vervaele (eds.), *Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with other EU law enforcement* authorities *(ECN/ESMA/ECB)*, 2017, available at <https://dspace.library.uu.nl/handle/1874/352061> accessed 2 November 2023.
30 For more details on this argument see: S. Tosza, (2021) *Computer Law & Security Review, op. cit.* (n. 13), 10.
31 CJEU, 15 September 2022, Case C-419/14 (*WebMindLicences*); see also F. Giuffrida and K. Ligeti (eds.), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, 2019.
32 See supra note 17.
33 A. Frunza-Nicolescu, "Electronic Evidence Collection in Cases of the European Public Prosecutor's Office", in this issue.
34 It is unclear how to interpret Art. 31 of the EPPO Regulation in this context; in particular, Art. 31(6) seems to be inapplicable as its first condition is in contradiction with the last condition of Art. 5(2) of EPOR.
35 Art. 4 OLAF Regulation.
36 See in this regard, A. Weyembergh and C. Brière, *The future cooperation between OLAF and the EPPO*, In-depth Analysis for the CONT Committee, 2017.
37 Art. 14 OLAF Regulation.
38 Art. 101(4) EPPO Regulation.
39 Art. 101(3) EPPO Regulation and Art. 12e OLAF Regulation.
40 M. Simonato, M. Luchtman and J. Vervaele (eds.), *Exchange of information with EU and national enforcement authorities: Improving OLAF legislative framework through a comparison with other EU authorities (ECN/ESMA/ECB)*, 2018, available at: <https://dspace.library.uu.nl/handle/1874/364049> accessed 2 November 2023.
41 See, e.g., ECA Special Report 01/2019 on fighting fraud.
42 See, e.g., OLAF Report 2021.
43 See e.g., P. Mathiessen et al. "Misuse of EU-funds: Messerschmidt's foundations investigated for fraud", *European Press Prize*, <https://www.europeanpressprize.com/article/misuse-eu-funds-messerschmidts-foundations-investigated-fraud/> accessed 2 November 2023.
44 See European Commission, News Article of 2 October 2021, "European Blockchain Pre-Commercial Procurement", <https://digital-strategy.ec.europa.eu/en/news/european-blockchain-pre-commercial-procurement> accessed 2 November 2023.
45 Art. 7 OLAF Regulation.
46 While the CJEU has consistently considered OLAF's investigative measures to be preparatory measures, because they do not bring about a distinct change in the legal position of the person concerned, and thus regarded them as non-reviewable under Art. 263 TFEU, the Court could be called on to indirectly review such acts in the context of an action against the final measure adopted by the Commission (See CJEU, 19 December 2012, C-314/11 P, *Planet v Commission*) or alternatively through a preliminary question of validity under Art. 267 TFEU, when and if a decision is adopted by a national authority (but it requires that national courts refer questions to the Court, and there seems to be no references so far, which would call into question the legality of OLAF's investigative acts). See K. Bovend'Eerdt, *The Protection of Fundamental Rights in OLAF Composite Enforcement Procedures*, 2024 (forthcoming); M. De Bellis, "Multi-level Administration, Inspections and Fundamental Rights: Is Judicial Protection Full and Effective?", (2021) *German Law Journal*, 416-440. See also J. Inghelram, "Judicial review of investigative acts of the European Anti-Fraud Office (OLAF): A search for a balance", (2012) *Common Market Law Review (CMLR)*, 601.
47 Art. 12a OLAF Regulation.
48 See Art. 101(3) EPPO Regulation.
49 Art. 9 OLAF Regulation.
50 See Art. 9a OLAF Regulation.
51 Art. 15 OLAF Regulation.
52 A significant body of knowledge was assembled in number of projects as regards the gathering of electronic evidence, including exploring national law in many EU and third countries, e.g., JUD-IT (Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU) conducted by the Centre for European Policy Studies (CEPS) (cf. S. Carrera and M. Stefan, *Access to Electronic Data for Criminal Investigations Purposes in the EU*, 2020, Centre for European Policy Studies (CEPS), <https://www.ceps.eu/wp-content/uploads/2020/02/LSE20120-01_JUD-IT_Electronic-Data-for-Criminal-Investigations-Purposes.pdf> accessed 2 November 2023); DEVICES project (Digital forensic Evidence: towards Common European Standards in antifraud administrative and criminal investigations) conducted by the University of Bologna (cf. M. Caianiello and A. Camon (eds.), *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations,* 2020.), and the project "Cooperation of service providers in criminal investigations" (IC-TCOOP) conducted by the University of Liège. The results of this last project will be published in the Cambridge Handbook of Digital Evidence in Criminal Matters edited by V. Franssen and S. Tosza, 2024 (forthcoming).
53 Gathering electronic evidence for administrative investigations. Comparative study of law and practice (ELEVADMIN), financed by the Union Anti-fraud Programme (EUAF), Project: 101101776 — 2022-LU-ELEVADMIN. The author is the Coordinator and Principal Investigator of this project.
54 See, in detail, S. Tosza, (2023) *European Data Protection Law Review*, *op. cit.* (n. 24).

# Mutual Admissibility of Evidence and Electronic Evidence in the EU

## A New Try for European Minimum Rules in Criminal Proceedings?

Lorena Bachmaier Winter

**This article seeks to provide arguments in support of legislative action on mutual admissibility of evidence and electronic evidence in criminal proceedings at the EU level. To this end, it will first describe the status quo and then the main features of a corresponding proposal recently tabled by the European Law Institute. In the light of this proposal, the author explains why Member States should reconsider their traditional stance against any EU initiative on evidentiary rules in criminal proceedings. Ultimately, especially in this new digital era, the best solution to prevent the inadmissibility of cross-border evidence is to adopt a set of minimum rules.**

### I. Introduction

Judicial cooperation in criminal matters in the EU is based on the principle of mutual recognition. To this end, Art. 82 (1) and (2) of the Treaty on the Functioning of the EU (TFEU) establishes the competence of the EU to adopt measures and minimum rules in order to implement this principle, while respecting the possibility for Member States to maintain a higher level of protection of fundamental rights. On the basis of this legislative power, the EU has already adopted numerous directives and regulations to facilitate the principle of mutual recognition, e.g. on procedural rights, conflicts of jurisdiction, or victims' rights, to name but a few. Although Art. 82 (2) lit a) TFEU expressly mentions the possibility to adopt by means of directives rules on "mutual admissibility of evidence between Member States" to the extent "necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension", the EU has not yet adopted any legislative instrument in this regard.

Law enforcement authorities, public prosecutors, defence lawyers, and legal scholars have consistently argued that it is necessary to provide legal certainty in this area, not only to ensure the admissibility of cross-border evidence but also to provide for an adequate protection of the defendants' rights when faced with incriminating evidence obtained abroad.[1] The EU institutions have also acknowledged the need for such a legal framework,[2] but have so far failed to put forward a proposal on rules on the admissibility of evidence in criminal proceedings.[3] This does not mean that efforts to move forward in this field since the Tampere Council[4] have been lacking,[5] but it seems that the EU has not managed to gain enough support from Member States to put this topic on the agenda.

On 5 May 2023, the European Law Institute (ELI) adopted a Proposal for a Directive of the European Parliament and of the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings (hereinafter the ELI Proposal), which is the result of a two-year project.[6] It is a draft that is intended to serve as a blueprint for a future Directive on the admissibility of evidence in criminal proceedings. It has been discussed with all the main stakeholders involved in cross-border criminal proceedings in the EU, who have worked together to address and balance the needs and interests of all parties. It would be welcome if the EU Commission would use it as a starting point to move towards rules on the admissibility of evidence in transnational criminal proceedings.

But is there really a chance for a future Directive on admissibility of evidence? Do the differences in the legal traditions and in the national criminal justice systems prevent the adoption of certain minimum rules on admissibility of evidence?

This article seeks to address these questions and put forth arguments in favour of a legislative action at the EU level. I am convinced that the best way to prevent the inadmissibility of cross-border evidence lies in the adoption of a set of minimum rules, especially with regard to the new digital era in which we live. In the light of the ELI Proposal on the admissibility of evidence, I will outline why Member States should

reconsider their traditional negative stance against any EU initiative on evidentiary rules in criminal proceedings.

## II. The Main Features of the European Law Institute Proposal

Clear progress has been made in European judicial cooperation in criminal matters, which has mainly focused on simplifying procedures based on the principle of mutual recognition, restricting refusal grounds, establishing time frames for the execution of requests providing standardised forms, setting up swift communication among judicial authorities, etc. However, no parallel effort has been made to adopt general rules setting out the main principles on the admissibility of cross-border criminal evidence.[7] Said ELI Proposal seeks not only to fill this gap but also to provide certain standards for harmonising the gathering of electronic evidence. Keeping these two goals in mind, the ELI Proposal is divided into two parts.

The first part (Chapter 2) contains a set of rules aimed at clarifying which standards need to be respected in criminal proceedings when evidence has been gathered in another Member State under rules that are likely to be different from those applicable in the forum State. The ELI Proposal neither imposes rules on how the evidence should be gathered in each Member State nor stipulates how Member States are to regulate any of the criminal investigative measures (except certain rules regarding electronic evidence). It also does not affect the free assessment of evidence that lies with the national courts.

The principles set out in the first part try to balance the two main interests at stake: enhancing respect for defendants' rights, on the one hand, and enhancing the free circulation of evidence and therefore the effective prosecution of cross-border crimes, on the other. To this end. the Proposal establishes compliance with lex loci regit actum as the main principle (Art. 4 ELI Proposal); it is up to the executing authorities and for the trial court in the forum state to verify that these rules have been complied with. In addition, the defence shall have access to the necessary means to be able to verify whether the evidence gathered abroad has in fact been obtained in accordance with the lex loci. This principle is not new, since it is already set out in most MLA conventions.

What the ELI Proposal requires is that the lex loci regit actum principle is effectively complied with: the trial court, together with the executing authorities and the defence, has the duty to make certain that the evidence has been obtained in conformity with the lex loci. Ensuring adherence to the lex loci serves two goals: first, it is a requirement for the admissibility of evidence providing for lawfulness in the gathering of the evidence; second, it ensures that the diverse legal frameworks do not represent an obstacle to the admissibility (use) of the evidence obtained abroad. The only exception to this general principle is for cases in which the use of such evidence would infringe fundamental constitutional principles of the forum State (Art. 4 (1) ELI Proposal).

In this way, the ELI Proposal underlines that mutual recognition is not equivalent to applying the principle of non-inquiry. It aims at strengthening the principle of mutual recognition but only when the evidence has been lawfully obtained according to the *lex loci.* And this principle also applies to evidence obtained in administrative proceedings. It provides for some flexibility, however, allowing the forum State to activate a kind of emergency break and refuse the cross-border evidence if, despite complying with the *lex loci*, a fundamental principle of its constitution is violated.

Although this approach may not be ideal purely from the perspective of the principle of mutual recognition, it seems to be the most reasonable approach in order to help reduce Member States' resistance towards the adoption of a Directive on the admissibility of evidence. Knowing that there is still a possibility to invoke fundamental principles of the national justice system against the evidence obtained abroad should calm the existing concerns expressed by several national authorities.

In this realm, the problem of identifying the *lex loci* with regard to electronic evidence arises, as the location of the items of evidence is unknown in many cases. Art. 2 ELI Proposal clarifies this issue by defining the *lex loci* as the "place where the access to evidence was granted".

Evidence obtained by means of torture or ill-treatment, in violation of the right against self-incrimination, and by deception are considered grounds for the absolute inadmissibility of evidence (Art. 5 ELI Proposal). This neither represents an innovation nor an intrusion into the national criminal justice systems but simply a way of ensuring an effective respect for the fundamental rights standards in the Charter of Fundamental Rights of the European Union and in the European Convention on Human Rights (ECHR), as defined in the respective European courts' case law. Some argue that such an inadmissibility ground does not provide any added value, since such obligations already exist under the EU Charter and the CoE Convention. However, practice shows that the implementation of these standards is still far from being a reality in all Member States.

Art. 6 ELI Proposal provides for a set of non-absolute rules on the admissibility of evidence, whereby the Member States "shall ensure" that certain evidence is not admitted. This provision seeks to strengthen compliance with safeguards that are already included in most – if not all – national codes of criminal procedure such as the protection of the lawyer-client privilege.[8]

The second part of the ELI Proposal aims at providing precise rules on the gathering of electronic evidence.[9] These rules are mainly based on the already adopted international forensic standards as accepted in judicial practice.[10] This part includes safeguards to ensure the integrity, authenticity, and completeness of the electronic evidence, the possibility to challenge such evidence, and access to the IT expertise and other machine-learning devices – also for the defence (Art. 7 (5) ELI Proposal). Although no harmonising rules have been established for other types of evidence, there were two reasons for including very precise rules on the gathering of electronic evidence: first, the rules on gathering electronic evidence in criminal proceedings are at an incipient stage; second, such rules have not always been sufficiently developed in national legal frameworks.[11]

Lastly, the ELI Proposal establishes the need to provide for effective judicial remedies against the use of evidence obtained in breach of the rules set out in the proposed Directive (Art. 10). It also clarifies what the consequences of finding cross-border evidence inadmissible should be (Art. 11).

Having summarised the main features of the ELI Proposal for a Directive on mutual admissibility of evidence and electronic evidence in criminal proceedings, I will now put forth arguments as to why the Member States and the EU should favour the advancement of regulating admissibility of criminal evidence by way of a Directive.

## III. A Move towards a Directive on Admissibility of Cross-Border Evidence

For a long time, the EU has been aware of the need to set common rules or principles on the admissibility of criminal evidence. This is the reason why this topic is expressly mentioned in Art. 82 (2) lit. a) TFEU and why there have been continuous efforts to bring it to the attention of the Member States. Thus, it is out of the question that rules on the admissibility of cross-border evidence are needed.

The increased relevance of cross-border electronic evidence in practice underpins this need. More certainty is necessary to define in which cases and under which conditions electronic evidence obtained/accessed in another country will ultimately be admitted or refused as evidence in the forum State. The defence counsel faces the same uncertainty as the prosecution in many cases, since it is impossible to check how the electronic evidence was extracted from a device, how it was stored, which keywords or selectors were used during the search of a computer, or what the means were to transfer such data from one country to the forum State.

The present situation is clearly not compatible with a common Area of Freedom, Security and Justice (AFSJ): it neither provides for the free circulation of evidence nor does it promote security, as it poses obstacles to the effective prosecution of cross-border crime. In the end, it does not serve justice, as the defendant is confronted with evidence which he/she cannot challenge because either the principle of non-inquiry is applied or because he/she does not have means to find out how the evidence was obtained abroad. The need for European rules on the admissibility of criminal evidence should therefore no longer be debated: it should be agreed that it is necessary.

Considering the agreement on the need for a Directive on admissibility of evidence, why has there been so little progress in this regard? Of course, it is known that the EU's legislative processes are complex and that finding consensus on certain topics can be quite a challenge. The rules on admissibility of criminal evidence are not an exception. This is also true, however, for many other topics and issues, which have nevertheless gone through the EU legislative process and eventually become EU law. There must be other reasons to explain the lack of advancement in the area of admissibility of evidence.

At present, the European Commission claims that the war scenario in Ukraine and the need to protect victims as well as secure evidence of war crimes related to the Russian invasion are to be the absolute priority in the field of justice and home affairs. On the one hand, this is completely justified because there is no question that discussing the rules on admissibility of criminal evidence is clearly not a priority compared to the challenges arising from the war. On the other hand, this is not convincing, since the EU has always been able to work on several fronts and make progress in areas seen as necessary, albeit not as a high priority on the agenda.

This being said, it appears that the Member States – convening in the Council – are not motivated to tackle the issue of admissibility of evidence, considering that any EU law in

this area would cause unwelcome meddling in the respective national criminal justice system and its own internal balances. The traditional resistance of the Member States to EU law in the area of criminal law –still considered one of the areas most closely linked to their sovereignty – also plays a role in this context.

This resistance would be understandable if the premise were correct, if there were rules that would interfere with the sovereignty of the Member States, if the EU law intended to stipulate how national judges should decide on the admissibility of evidence or which exclusionary rules of evidence should be applied. The opposition would also be justified if the interference in the national criminal justice systems was illegitimate. However, a closer look at the ELI Proposal shows that this is not the case: the ELI Proposal neither imposes additional exclusionary rules nor does it add new principles to the admissibility of evidence. Rather, it tries to balance the interests at stake by seeking a better implementation of the existing rules and international standards.

In this context, it must be called to mind that the ELI Proposal is not a merely theoretical academic exercise but instead the result of numerous discussions and compromises among all the stakeholders, as practitioners have been as involved in its drafting as scholars. The ELI Proposal therefore does not take a unilateral stance in favour of the prosecution or the defence, and perhaps this balanced approach is the reason why no one is completely satisfied with the result, even though all stakeholders tend to agree that it improves the present uncertain situation.

The task of the drafters has been to find solutions that promote the effective prosecution of crime by facilitating not only the access to cross-border evidence but also the possibility to use it later at trial. At the same time, the drafters aimed to avoid the cross-border element of the evidence from ending up lowering the safeguards of the defence rights. Preventing the defence from challenging the lawfulness of the evidence gathered abroad – by way of procedural rules or by way of practical impossibility or lack of resources – is not an adequate way to move towards a more effective prosecution at the cross-border level in the AFSJ.

Moreover, the standards on the admissibility of evidence reflected in the ELI Proposal have already been defined in the case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). No additional exclusionary rules that would interfere with the general structure and principles of national criminal proceedings were introduced; thus, it would be most awkward for anyone to oppose the implementation of rights already defined for which compliance is already an obligation. In other words, opposing an EU legislative instrument on admissibility of criminal evidence like the ELI Proposal would run counter to strengthening the rule of law in the EU.

All these reasons should not only help allay the Member States' fear of EU law being adopted in the field of admissibility of criminal evidence but also encourage them to support a reasonable legislative initiative in this area.

## IV. Time to Ban the Principle of Non-Inquiry in Cross-Border Evidence

It is conventionally put forward that it is not feasible to control respect for the *lex loci* (before transferring evidence and admitting it as incriminating evidence at trial in the forum State), as proposed by ELI. It is argued that it is not possible for the trial court to verify whether the gathering of evidence in a foreign country was carried out with respect for the law applicable in that country, given that the court does even not know which law is to be applied. Even though such an argument might be justified because the maxim *iura novit curia* does not apply to foreign law, it is not an indisputable one. There are many ways to ensure that evidence obtained abroad is compliant with the *lex loci,* which do not necessarily require the forum judge to become an expert in foreign law, e.g. calling in a foreign lawyer to give an expert opinion, allowing the defence to hire a lawyer in the foreign country where the evidence was obtained, requiring the law enforcement authorities to describe in detail how the piece of evidence was gathered –as it is done in practice in EPPO proceedings when cross-border evidence is gathered by the assigned European Delegated Prosecutor–. In sum, while the argument based on the principle of non-inquiry may have been justified in the pre-digital area, in today's world of fluid communications and easy access to legal information from a foreign country, it is high time to adapt the standards on admissibility of cross-border evidence to this new global scenario. As a consequence, sticking to the principle of non-inquiry is simply not acceptable within the EU's AFSJ. In addition to the lack of logic as to the principle of non-inquiry in a digital global society, a ban on this principle is also called for because it lowers the rights of the defendant, who would be deprived of the possibility to challenge the lawfulness of the cross-border evidence.

It could be argued that the principle of non-inquiry is the expression of the mutual recognition principle, given that it

is based on the premise that all national authorities comply with the law, also when gathering evidence. I do not aim here to put into question the professionalism and trustworthiness of the public authorities carrying out a criminal investigation and conducting investigative measures. However, the core issue remains that, despite the mutual trust between public authorities, the defence has still the right to check how the evidence has been gathered abroad, and it is the duty of any defence lawyer to ensure that this has been done in compliance with the procedural rules. This is how the adversarial procedure works, and this principle is to be respected regardless of whether the defence is confronted with evidence obtained in the forum State or in another EU Member State.

One primary rule for the fairness of the proceedings (Art. 6 ECHR) is that the evidence must have been lawfully obtained. The consequences of an infringement of these rules might diverge – strict exclusionary rule or balancing test –,[12] but it cannot be denied that lawfulness is a principle to be followed in the obtaining of criminal evidence. Thus, it seems only logical that it should be controlled by the trial court and that the defence should be allowed to control it as well. Once there is agreement on this main condition, it can be discussed how this control should be carried out, and what the consequences of a violation of the *lex loci* principle should be.

At this point, the ELI Proposal does not aim for a drastic solution, such as excluding any evidence that does not adhere completely to the *lex loci.* It only provides for the absolute exclusion of evidence in the same cases in which the ECtHR has already determined that such methods of obtaining evidence are contrary to the ECHR (torture, ill-treatment, deception, disproportionate coercion, and violation of the right against self-incrimination). For other breaches of the law and violations of so-called "derogable" fundamental rights, the ELI Proposal seeks in its Art. 6 to enhance the level of safeguards by which Member States "shall ensure that such evidence is not admitted". This means that the national procedural rules must foresee ways of checking the legality of such evidence, including for the defence.

However, this provision does not create new exclusionary rules or requirements for the admissibility of evidence that are not already envisaged at the national level. For example, the protection of immunities, which has been included in Art. 6 ELI Proposal, merely reflects what has already been foreseen in all national codes of procedure of the Member States. Including these immunities in an EU Directive will only grant them an enhanced protection by stipulating that such cross-border evidence should not be admitted. In sum, the model proposed by the ELI would also stand against arguments that it would alter the procedural models of a country or against objections raised on the basis of the inquisitorial nature or other features of a national criminal procedure.

## V. Common Standards on the Gathering of Electronic Evidence

Ultimately, Member States often argue against the harmonisation of the rules on investigative measures and evidence gathering by asserting that the investigative measures, especially those that are coercive or restrictive to fundamental rights, are closely linked to the national understanding of the principle of proportionality and national values.

However, this argument is not strictly applicable when it comes to electronic evidence. Most countries do not have a precise regulation on the gathering of this type of evidence. In fact, as the drafters of the ELI proposal explain,[13] the complete absence of rules at the national level is both a shortcoming and an advantage: a shortcoming, as it does not provide legal certainty at the national level but an advantage because the lack of existing rules facilitates the adoption of international standards and therefore the rules contained in a (future) EU Directive, as they would not generally conflict with any national rules or principles.

In view of a future EU legal framework, it should also be borne in mind that, in the area of electronic evidence, IT experts and lawyers have been developing detailed international forensic standards precisely to fill the legal gap.[14] Since electronic evidence has a cross-border dimension in a vast number of cases, the need to harmonise the rules for its gathering is even greater than for physical evidence. The volatile nature of electronic data requires a series of safeguards to be adopted from the very beginning of the procedure involving access to them, in order to ensure that the electronic evidence will not be subject to manipulation and to establish that it is authentic.

For these reasons, action at the EU level ensuring admissibility of electronic evidence is more necessary than ever. The setting of these common rules would not only enhance the rights of the defence but also the effectiveness of the prosecution, avoiding the risk that electronic evidence is ultimately not admissible, for example because the chain of custody has been broken. Again, I do not see why Member States would seek to oppose what would entail an advantage for the effective prosecution of crime, while ensuring compliance with fundamental rights.

## VI. Conclusion

The analyses in this article have demonstrated that there is a need to convey the message that defining a clearer legal EU framework on admissibility of evidence will benefit all parties involved in criminal proceedings: the prosecution, victims, and the defence. More legal certainty and a uniform approach towards the principles on admissibility of cross-border evidence in a common Area of Freedom, Security and Justice are not only requirements for an efficient cross-border prosecution of crime but also signify the commitment of all EU Member States to the fairness of criminal proceedings.

Agreeing on common minimum standards for the gathering and transmission of evidence, including a set of minimal conditions for the admissibility of evidence, while taking into account the differences between the legal traditions and systems of the Member States is vital in order to safeguard fundamental rights and facilitate judicial cooperation at the EU level. And the digital revolution has definitely increased the need for such common minimum rules.

The ELI Proposal on mutual admissibility of evidence and electronic evidence in criminal proceedings outlined here has not only been designed to raise awareness on this issue but could also be taken as a launchpad for further developing EU law on admissibility of criminal evidence. This has been demanded by practitioners for a long time. The intensive supranational work by the European Public Prosecutor's Office also speaks for immediate legislative action in this area.

**Prof. Dr. Lorena Bachmaier Winter**
Full Professor of Law, Complutense University Madrid (UCM)

1 Another issue that should be addressed in the future is whether the proposed rules on the admissibility of evidence should cover only cross-border evidence or also apply to purely domestic cases, avoiding thus unequal treatment between the level of protection of the rights of defendants when facing a cross-border case or a domestic one. See J. A. E. Vervaele, "Lawful and fair use of evidence from a European human rights perspective", in F. Giuffrida and K. Ligeti (eds), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, 2019, p. 56.

2 See, *inter alia*, Commission of the European Communities, "Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen", COM(2009) 262 final.

3 Although Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters and Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office mention the issue on admissibility of evidence and include provisions to facilitate it, they do not provide rules.

4 See, among others, European Council of 15-16 October 1999, "Conclusions of the Presidency", SN 200/1/99 REV 1; the Programme of measures to implement the principle of mutual recognition of decisions in criminal matters, *O.J.* C 12, 15.1.2001, 10; Commission of the European Communities, "Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility", COM(2009) 624 final.

5 Cf, for instance, Milieu, *Study on Cross-Border Use of Evidence in Criminal Proceedings. Final Report*, March 2023, study upon the request of the Directorate-General Justice and Consumers, available at: <https://op.europa.eu/en/publication-detail/-/publication/2815b94e-9165-11ed-b508-01aa75ed71a1/language-en/format-PDF/source-291553958> accessed 2.11.2023.

6 The text of the ELI Proposal is available at: <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf> accessed 2.11.2023.

7 On transnational evidence in the EU, see, *inter alia*, A. van Hoek and M. Luchtman, "Transnational Cooperation in Criminal Matters and the Safeguarding of Human Rights", (2005) 1 (2) *Utrecht Law Review* 1–39, 15; S. Allegrezza, "Critical Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from one Member State to another and Securing its Admissibility", (2010) 9 *ZStW*, 573; S. Ruggeri, "Introduction to the Proposal of a European Investigation Order: Due Process Concerns and Open Issues", in S. Ruggeri (ed.), *Transnational Evidence and Multicultural Inquiries in Europe,* 2014, 29–35; L. Bachmaier Winter, "Transnational Criminal Proceedings, Witness Evidence and Confrontation: Lessons from the ECtHR's Case Law", (2013) 9 *Utrecht Law Review*, 126–148; L. Bachmaier Winter, "Transnational Evidence: Towards the Transposition of the Directive 2014/41 Regarding the European Investigation Order in Criminal Matters", (2015) *eucrim*, 47–59; C. Claverie-Rousset, "The admissibility of evidence in criminal proceedings between European Union Member States", (2013) *EuCLR*, 152–169; K. Ligeti, B. Garamvölgyi, A. Ondrejova, and M. Gräfin Von Galen, "Admissibility of evidence in criminal proceedings in the EU", (2020) *eucrim*, 201–208.

8 Art. 6 of the ELI Proposal is entitled "*Non-absolute inadmissibility of evidence*" and reads as follows:
(1) Member States shall ensure that self-incriminating statements by the suspect during police interrogations in the absence of a defence lawyer are not admitted as evidence unless the defendant confirms them at trial.
(2) Member States shall ensure that evidence obtained in breach of the right to confidentiality of communications with the defence counsel is not admissible in criminal proceedings.
(3) Member States shall ensure that evidence concerning communication with clergymen obtained in violation of the seal of secrecy is not admissible in criminal proceedings.
(4) The obligations under paragraphs 2 and 3 shall not apply if the person to whom the confidential information is communicated is

suspected of being involved in the criminal offence which is the subject of the proceedings.
(5) The obligations under paragraphs 1 to 4 shall also apply with respect to the evidence obtained in administrative proceedings.
9 For details, see Explanatory Memorandum of the ELI Proposal, p. 16.
10 In the Explanatory Memorandum of the ELI Proposal, the forensic standards which are mentioned as generally accepted are: The 2019 Interpol "Global Guidelines for Digital Forensics Laboratories" (<https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf>); ENFSI, "Best Practice Manual for the Forensic Examination of Digital Technology" of 2015 (<https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf>); and International Organization for Standardization (ISO), "SO/IEC 27037:2012, Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence" (<https://www.iso.org/standard/44381.html#:~:text=ISO%2FIEC%2027037%3A2012%20provides,can%20be%20of%20evidential%20value>). All accessed 2.11.2023.
11 See Explanatory Memorandum of the ELI Proposal, p. 17.
12 See S. C. Thaman, "Balancing Truth Against Human Rights: A Theory of Modern Exclusionary Rules", in S. C. Thaman (ed), *Exclusionary Rules in Comparative Law,* 2013, 403–446. On the aims of the exclusionary rules see also the comparative study of S. Gless and T. Richter (eds.), *Do exclusionary Rules Ensure a Fair Trial? A Comparative Perspective on Evidentiary Rules,* 2019.
13 See Explanatory Memorandum of the ELI Proposal, p. 17.
14 See M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, 2021; S. Mason and D. Seng (eds.), *Electronic Evidence and Electronic Signatures*, 2021, available at: <https://humanities-digital-library.org/index.php/hdl/catalog/view/electronic-evidence-and-electronic-signatures/214/408> accessed 2.11.2023.

# Efficiency *contra legem*?

## Remarks on the Advocate General's Opinion Delivered on 22 June 2023 in Case C-281/22 G.K. and Others (Parquet européen)

Hans-Holger Herrnfeld

**The first preliminary ruling request concerning the EPPO Regulation raises several interesting questions regarding the interpretation of its Art. 31 on cross-border investigations. Advocate General *Ćapeta* presented her Opinion and proposals to the Court of Justice of the European Union on 22 June 2023. Her analysis shows the difficulties that the Court will presumably face when trying to find proper answers to the questions raised by the Higher Regional Court of Vienna (Austria), as it is difficult to reconcile the wording and context of its provisions and its legislative history with the Union legislator's presumed objectives, namely, to establish an efficient system for cross-border cooperation. The author concludes that a proper solution will in any case require an amendment of Art. 31 by the Union legislator. In particular, it should be up to the legislator to clarify the scope of review to be undertaken in the course of any ex ante judicial authorisation to be obtained in the Member State in which the ordered investigation measure is to be executed.**

### I. Introduction

It came as no surprise that the provisions of Art. 31 of Regulation (EU) 2017/1939 (hereinafter: EPPO Reg.)[1] on cross-border investigations within the EPPO's territory would become subject to one of the first references for a preliminary ruling to the Court of Justice of the European Union (hereinafter "ECJ" or "Court"). The negotiations on this provision had been particularly controversial in the Council, and the resulting text of Art. 31 is not very convincing.[2] The main question heavily debated at the time was whether a required judicial authorisation of an investigation measure in a cross-border setting should be obtained from a court/judge in the Member State in which the investigation is being conducted or in the Member State in which the requested investigation measure is to be undertaken. While the EPPO has been conceived as a "single office" (Art. 8(1) EPPO Reg.), it nevertheless operates on the basis of national criminal procedural law (cf. Art. 5(3) EPPO Reg.) and thus not in a "single legal area".[3] The rules on cross-border investigation measures by the EPPO thus need to clarify which national legal regime is to apply and in which Member State judicial authorisation is to be obtained.

In January 2022, the College of the EPPO considered it appropriate to issue internal guidelines[4] on the interpretation of Art. 31 and the procedures to be kept when the European

Delegated Prosecutors (hereinafter: EDPs) request the judicial authorisation of an investigation measure, essentially requiring the EDPs to obtain a required judicial authorisation in the Member State in which the so-called "handling EDP" conducts the investigations. While the interpretation given by the College may be debatable as such a rule is at least not specifically set out in Art. 31, the guidelines offer a pragmatic interpretation of the EPPO Regulation until the Council perhaps decides to amend and/or clarify the text of Art. 31.

Before the College adopted the guidelines, however, the question of interpretation of Art. 31 had already become an issue in proceedings before the Higher Regional Court of Vienna, Austria *(Oberlandesgericht Wien)*. The Vienna court considered it necessary to request a preliminary ruling from the European Court of Justice (reference: Case C-281/22). A hearing in that case was held on 27 February 2023 and Advocate General (AG) *Tamara Ćapeta* presented her Opinion on 22 June 2023.[5]

This article provides a summary of the Advocate General's Opinion, analyses its findings, and offers possible conclusions prior to rendering of the ECJ judgment, which is expected to follow by the end of 2023.

## II. Facts and Relevant Legal Framework

A German European Delegated Prosecutor ("handling EDP") investigated an alleged criminal offence, which required search and seizure measures *inter alia* in Austria. In accordance with Art. 31(3) subparagraph 1 EPPO Reg. as well as the German law implementing the EPPO Reg.,[6] the German EDP did not obtain judicial authorisation in Germany for the searches/seizures to be conducted in Austria (which would have been required in a domestic case in Germany). The reason was that, in accordance with Austrian law, a prior judicial authorisation for such measure is necessary and thus – in accordance with Section 3(2) of the German implementing law – no judicial authorisation in Germany was required. The German EDP assigned the measure to his Austrian colleague ("assisting EDP") who obtained search and seizure warrants from Austrian courts. Subsequently, the defendants filed an appeal against the search warrants before the Higher Regional Court of Vienna. In their view, the measures were neither necessary nor proportionate. In the course of the proceedings, the Austrian EDP claimed that, in accordance with the EPPO Regulation, the justification of the measure may be examined only in the Member State of the handling EDP. In his opinion, the court in the assisting EDP's Member State cannot assess the substantive validity of the measures but may control only whether the measure complies with formal and procedural requirements. The Higher Regional Court of Vienna therefore presented three questions to the ECJ. While these questions focus on the scope of review to be undertaken by the court in the Member State of the assisting EDP, they are closely related to the underlying question of whether the substantive *ex ante* review to be undertaken in the course of a required judicial authorisation is a competence belonging to the court/judge in the Member State of the handling EDP (where the investigation proceedings are being conducted) or of the court/judge in the Member State of the assisting EDP (where the required measure is to be enforced).

The relevant legal framework is set out in Art. 31 EPPO Reg on "Cross-border investigations". Its paragraph 1 provides that the handling EDP "shall decide on the adoption of the necessary measure and assign it to a European Delegated Prosecutor located in the Member State where the measure needs to be carried out." Art. 31(2) concerns the "justification and adoption" of the measure by the handling EDP, and it applies irrespective of whether the adoption, in accordance with national law, requires a judicial authorisation or not. The second sentence reads as follows: "The justification and adoption of such measures shall be governed by the law of the Member States of the handling European Delegated Prosecutor." This is followed by paragraph 3 of Art. 31 on "judicial authorisation", which differentiates between situations in which judicial authorisation is required under the law of the assisting EDP's Member States (subparagraphs 1 and 2) and situations in which judicial authorisation is only required under the law of the handling EDP's Member State (subparagraph 3). Art. 31 is followed by Art. 32 EPPO Reg. entitled "Enforcement of assigned measures".

## III. Summary of the Opinion by Advocate General *Ćapeta* and Her Conclusions

In her Opinion, AG *Ćapeta* refers in detail to two very different understandings of Art. 31 EPPO Reg. The first one was put forward by the Austrian and German governments (referred to by the Advocate General as "Option One"), and the second one was submitted by the Commission and largely supported by the EPPO as well as the governments of Netherlands and Romania (referred to as "Option Two"). According to the views in favour of "**Option One**", it follows from the text of Art. 31(3) that, where a judicial authorisation is required under the law of the assisting EDP's Member State, this is to be obtained in that Member State. The judge/court of that Member State should undertake a full substantial review of the legality and proportionality of the requested

measure. The Austrian and German governments consider that the wording of Art. 31 is quite clear in this respect and "the courts cannot depart from it" (mn. 35 f.).[7] By contrast, the Commission and other proponents of "**Option Two**" argued: "if the law of the assisting EDP's Member State requires a judicial authorisation of an investigative measure, such an authorisation may entail only a review of the formal and procedural aspects relating to the execution of the measure (…). If the laws of the Member States of both the handling and the assisting EDPs require judicial authorisation, two authorisations are to be issued. The court of the handling EDP's Member State would authorise the measure if it finds it justified, whereas the court of the assisting EDP's Member State would authorise the procedural modalities of its execution." (mn. 38 f.).

In the introductory part of her Opinion, AG *Ćapeta* concludes that "none of the proposed outcomes are fully justified" under applicable interpretive techniques; "nevertheless, the Court will have to choose one." (mn. 4).

Before entering into an interpretation of the relevant provisions of Arts. 31 and 32, AG *Ćapeta* initially refers to the Austrian/German alternative proposal for what is now Art. 31(3) (mn. 27), which had been presented in the Council Working Group (COPEN) in April 2015 and reads as follows:

> Where a measure needs to be undertaken in a Member State other than the Member State of the handling European Delegated Prosecutor, the latter shall order the measure in accordance with the law of the Member State of the handling European Delegated Prosecutor and, where necessary, shall apply for a judicial authorisation thereof, or shall request a court order for the measure.

The Advocate General then rightly points out, that this proposal had failed to make its way into the final text of the EPPO Regulation (mn. 28). In her view, the final text of Art. 31(3) "does not clearly specify which Member State law determines whether prior judicial authorisation for executing a measure is necessary, nor which court is responsible for granting such authorisation." (mn. 29).

Nevertheless, she essentially follows the views of the Commission (mn. 73) that the solution proposed by Austria and Germany during the negotiations, according to which the handling EDP must obtain the necessary judicial authorisation in his/her own Member State, is exactly what Art. 31 now regulates in its paragraph 2, albeit in an imperfect way. Her further analysis then leads AG *Ćapeta* to conclude the following:

> Article 31(3) of the EPPO Regulation should be understood as allowing the court of the Member State of the assisting EDP to review only the aspects related to the execution of an investigative measure, while accepting the assessment by the handling EDP that the measure is justified, whether or not the latter is backed by prior judicial authorisation of the court of the Member State of the handling EDP. (mn. 73).

Furthermore, she points out that "the EPPO Regulation is indeed the most advanced piece of legislation yet …. The EPPO is a single body and the assigned cross-border measures indeed need not be recognised, but only implemented." (mn. 101).

## IV. Analysis

### 1. Interpretation of Art. 31 *contra legem*?

The Advocate General's Opinion correctly reflects that the Austrian and German governments substantiated their interpretation largely on the wording of the text as well as on the contextual relationship between paragraphs 2 and 3 of Art. 31, whereas the Commission and the EPPO placed a strong focus on the objectives of the Regulation to establish an efficient system for cross-border cooperation within the EPPO's territory. Much of the discussion at the hearing on 27 February 2023 did indeed circle around the question of whether the text of Art. 31 and the contextual position of its paragraph 3 are sufficiently clear and properly reflect the Union legislator's intention or whether the objectives aimed at by the legislator should primarily guide the interpretation of the text.

Referring to these different views, the Advocate General recalls an interpretative rule used by the ECJ according to which "where a provision of Community law is open to several interpretations, preference must be given to that interpretation which ensures that the provision retains its effectiveness." (mn. 64).[8] But is that really the case that Art. 31 is "open to several interpretations"? In respect of wording and context AG *Ćapeta* simply reflects the fact, that the proponents of "Option One" and "Option Two" offer two different interpretations of the text but she addresses the question of whether these different interpretations are both possible only in respect of the arguments put forward by Austria and Germany, namely that "Option Two" would render paragraph 3 of Art. 31 superfluous – an argument she, in conclusion, does not share (c.f. IV.2.b) below). Other than that, she apparently considers the interpretation offered by the proponents of "Option Two" to be "equally plausible" and thus concludes that, if the Court were to follow this interpretation, it "cannot be treated as a *contra legem* interpretation." (mn. 67).

On other occasions, however, the ECJ has also ruled that the interpretation of EU law requires that account be taken of the origins of the provision and "in particular regard should

be had to, inter alia, the recitals of the EU act concerned, since they constitute important elements for the purposes of interpretation, which may clarify the intentions of the author of that act."[9] As will be shown below, even if one considers both "Options" to be equally possible in terms of "text" and "context", the legislative history and recital 72 of the EPPO Regulation clearly indicate the legislator's intention and would allow an interpretation in accordance with "Option Two" only if one were to make the – presumed – objective of the provision, to establish an efficient system of cross-border investigation, the deciding factor for the interpretation.

## 2. Four interpretative methods applied

### a) Textual interpretation

The Advocate General observes that both proponents of both "Options" agreed on one issue: paragraph 3 subparagraph 1 of Art. 31 applies in situations in which judicial authorisation is required under the law of both, the handling EDP's Member State and the assisting EDP's Member State; and it also applies where judicial authorisation is required only under the law of the assisting EDP's Member State. Subparagraph 3 of that provision – in turn – applies where only the law of the handling EDP's Member State requires judicial authorisation (mn. 42 to 44).

The Austrian and German governments interpret Art. 31(2) to clearly determine that the adoption and justification of the measure by the handling EDP is governed by the law of that Member State, whereas paragraph 3 specifies where a necessary judicial authorisation for ordering the measure would need to be obtained (mn. 43 f.), i.e. which court is expected to undertake a full *ex ante* review of the measure in terms of the necessary level of suspicion, proportionality, etc. as required under national law (mn. 35).

According to the Commission's view, the judicial authorisation to be obtained by the handling EDP (conditions set out in national law, sufficient grounds/justification of the measure) is covered by Art. 31(2) (mn. 50), whereas Art. 31(3) does not at all concern substantive issues relating to the legality of the investigation measure but only the judicial authorisation of the "mode of execution of the requested investigative measure and not its justification" (mn. 53), i.e. only "procedural modalities of its execution." (mn. 39).

It remains unclear, however, why the Commission considers the text to say so. In the course of the hearing, the Commission at least conceded that it would have been preferable had the legislator clarified the text by inserting in Art. 31 paragraph 3 the words "of the enforcement" after "judicial authorisation". But the legislator did not do so – perhaps because this was not what the legislator actually had in mind (c.f. IV.2.d) below); in addition: the enforcement of the assigned measure is specifically regulated in Art. 32. It also remains rather unclear what exactly the "judicial authorisation of the enforcement of the measure" is supposed to mean in practice. This is also not clarified in the Opinion given by AG *Ćapeta*. In her view, the EPPO is "a single body and the assigned cross-border measures indeed need not be recognised, but only implemented." (mn. 101). Thus the "judicial authorisation of the enforcement of the measure" apparently would have to be something different (less?) than the role of the courts described in Art. 9 of the EIO Directive[10]. Furthermore: What would – in the views of the Commission and the Advocate General be the purpose of the second subparagraph of Art. 31(3) according to which the handling EDP, if "judicial authorisation for the assigned measure is refused, … shall withdraw the assignment"? If this judicial authorisation only concerns certain "modalities" of the enforcement, why should the handling EDP then be obliged to withdraw the assignment?

The Advocate General reflects the Commission's view of the purpose of the third subparagraph of Art. 31(3), recalling that the Commission at the hearing acknowledged that the use of the word "however" in Art. 31(3), subparagraph 3 "complicates matters for the interpretation of Article 31(3) of the EPPO Regulation." (fn. 32 referred to in mn. 42). In the view of the Commission, where no judicial authorisation is required in the Member State of the assisting EDP, the judicial authorisation by the court in the Member State of the handling EDP shall cover both, "its justification and the execution of the measure." (mn. 45). That is also hardly convincing: If the execution (enforcement) of the measure is to be carried out in accordance with the law of the assisting EDP's Member State (c.f. Art. 32) and if that law does not provide for a need to obtain judicial authorisation of the enforcement, why then should the court in the handling EDP's Member State have to give judicial authorisation to the enforcement? And what would be the applicable law for such an authorisation?

Finally: if – in the Commission's views, the term "enforcement" is "missing" in paragraph 3: does that apply to both instances where the term "authorisation" appears in the first sentence of paragraph 3? In other words, does the rule set out therein apply where Member State law specifically requires the prosecutor to obtain judicial authorisation of the enforcement of the measure (its modalities etc.)? Or is – in the Commission's views– the word "enforcement" only missing in the second part of the first sentence so

that whenever national law of the assisting EDP's Member States provides for judicial authorisation to order the measure (substantial grounds), the court now has to authorise the enforcement of the measure (modalities) only?

### b) Context of the provision

In terms of context, the Advocate General refers to the views expressed by the Austrian and German governments that the third subparagraph of Art. 31(3) would be obsolete, if one were to follow the interpretation offered by the Commission: there would be no reason to regulate here the exceptional role of the court in the handling EDP's Member State if – as the Commission suggests – the judicial authorisation by a court in that Member State is to be undertaken on the basis of Art. 31(2) and the enforcement is regulated in Art. 32. AG *Ćapeta* here also refers to the views expressed by the Austrian and German governments that recital 72 of the Regulation clearly expresses the intention of the legislator according to which "there should be only one authorisation." (mn 48).

Furthermore, AG *Ćapeta* refers to the view of the Commission that it is precisely the relationship between paragraphs 2 and 3 that actually confirms the interpretation according to which paragraph 2 also concerns the judicial authorisation by the court in the handling EDP's Member State (mn. 50). In respect of recital 72, she points out that the Commission "acknowledged that the desire for a single judicial authorisation was not ideally expressed in Article 31…." (mn. 54).

In her own interpretation, AG *Ćapeta* states that the "most convincing argument … offered by the Austrian and German governments, is that Article 31(3) of the EPPO Regulation becomes obsolete under Option Two." (mn. 68). Nevertheless, she considers that its provisions "can be given a meaning beyond that of Article 31(2) and Article 32" and concludes (mn. 70) as follows:

> Expressing the rule relating to the law applicable to judicial authorisations separately might have been perceived as necessary, due to the difficulties that that precise issue presented during the legislative negotiations. The redundancy of Article 31(3) cannot thus be used as an argument against adopting Option Two.

This explanation, however, is hardly convincing: Why should the legislator have decided to include such a "redundant" provision only for purposes of clarification and then use such – apparently – unclear wording in paragraph 3 that it allows for "different and mutually exclusive interpretative outcomes" (mn. 41), which – according to the Advocate General – are "equally plausible" (mn. 67)? And why would the provision of paragraph 3 – if it really addresses only the judicial authorisation of the modalities of enforcement – be set out in Art. 31 rather than in Art. 32, which regulates the enforcement?

### c) Objectives pursued by the legislator

In terms of objectives, AG *Ćapeta* points out that Austria and Germany admitted that their interpretation of the Regulation may indeed lead to practical difficulties for the EPPO but that, unfortunately, their alternative proposal had not been accepted during the negotiation process (mn. 56). She then gives a detailed account of the view of the Commission and the other proponents of "Option Two", according to which "[e]fficiency should therefore guide the interpretation of Article 31 of the EPPO Regulation." (mn. 57).

The crux of the matter here is that the Council, or at least the majority of its members, of course intended to set up an efficient system of cross-border investigations. However, a large group of Member States wanted to base cross-border cooperation within the EPPO territory on the principles of mutual recognition (in particular the concepts of the EIO Directive), while others wanted a system that is "more advanced" than mere mutual recognition.[11] The solution for situations in which no judicial authorisation is required (Art. 31 paragraphs 5, 7, and 8) found consensus fairly quickly; this system clearly is designed to make cooperation easier than that provided for in the EIO Directive, as it neither foresees any need for the assisting EDP to "recognise" the assigned measure nor a possibility to "refuse" its enforcement. Instead, the EDPs are expected to consult each other; if they cannot reach an agreement, the Permanent Chamber decides.

By contrast, it was much more difficult to find consensus in the Council on the proper procedure when a judicial authorisation is required. This was not a question of whether the provisions in Art. 31 should establish an efficient system but how to achieve that. During the negotiations in the Council, some delegations – including Austria and Germany – raised concerns over the proposed solution that (full) judicial authorisation should always be obtained in the Member State of the assisting EDP; this was seen too cumbersome and overly time-consuming, because it may require presentation of the full case file, normally including a translation thereof.[12] The majority of delegations at the time, however, considered this risk neglectable and favoured the solution that had been drafted along the lines of the current text of Art. 31 EPPO Reg. A major concern for them was that there should always be only one judicial authorisation (cf. recital 72), as the involvement

of courts in two Member States would make the system overly cumbersome and time-consuming. In respect of the solution whereby judicial authorisation would have to be obtained from the court in the assisting EDP's Member State, the suggestion was made in the Council Working Group discussions that there should actually be no need to present the full case file to the court – including a translation thereof – but that a summary provided by the prosecutor should be sufficient for the court to undertake the substantial review.

### d) Legislative history

It is interesting to note what AG *Ćapeta* reveals in terms of the different views on the relevance of the regulation's legislative history. She recalls the position of the Austrian and German governments, which pointed out that the legislative history – as also reflected by a sequence of alternative draft texts discussed in the Council working parties – clearly confirms their interpretation of the text. By contrast, in respect of the Commission's standpoint, all that AG *Ćapeta* does – and presumably could – refer to is that the Commission claims to have changed its view in the course of history. At the hearing on 27 February 2023, the Commission had been confronted with the fact that the Commission's own legislative proposal of 2013[13] had already provided a solution, according to which *the only* judicial authorisation would have to be obtained in the Member State in which the investigation measure is to be enforced. AG *Ćapeta* reflects in the Opinion that the Commission gave as explanation the fact that in 2013 the EIO Directive had not yet entered into force. The Commission claimed that it had subsequently discovered that the EIO system works quite well and therefore "found it fortunate that the legislative institutions did not accept its original proposal that judicial authorisation ought to depend on the law of the Member State of the assisting EDP only, and instead have amended that proposal into what is today Article 31 of the EPPO Regulation…." (mn. 62).

In her own interpretation, AG *Ćapeta* mainly refers to said interpretative rule used by the ECJ, according to which "where a provision of Community law is open to several interpretations, preference must be given to that interpretation which ensures that the provision retains its effectiveness." That interpretative rule, in her view, favours Option Two (mn. 64). She then essentially advocates her interpretation of Art. 31 by stating that, if the ECJ were to follow the interpretation offered by Austria and Germany, this would "be seen as an invitation to the EU legislature to react", as it would "require an amendment of the EPPO Regulation to enable efficient cross-border investigations." (mn. 71).

A look at the legislative history of Art. 31 EPPO Reg. indeed explains the dilemma. During consecutive Council Presidencies in 2014 and 2015, different proposals for what is now Art. 31 (at that time first Art. 26a, later Art. 26) were discussed and discarded. In particular, the Austrian and German governments had provided a counter-proposal in April 2015,[14] according to which paragraph 1 was to specify that the handling EDP obtains any necessary judicial authorisation and submits this together with the assignment to the assisting EDP. Furthermore, in accordance with paragraph 5 of that proposal, the assisting EDP shall, where required, submit the order and, where applicable, the accompanying judicial authorisation to the competent court of his/her Member State for recognition. As mentioned before, and also properly reflected in the Advocate General's Opinion, this proposal did not meet with sufficient support in the Council Working Group.

In June 2015, the Latvian Presidency presented a compromise proposal,[15] which was drafted along the lines of what eventually became the final text of Art. 31. After further discussion, the ensuing Luxembourgish Presidency presented to the Council a document[16] containing two new alternative drafts: An "Option 1" provided that the handling EDP was to decide on the adoption and justification of the investigation measure in accordance with the law of that Member State (paragraph 2 of the proposal). And paragraph 4 of the proposal then stated that, if judicial authorisation of the assigned measure is required, "it can only be requested in the Member State of the assisting European Delegated Prosecutor". The underlying concept thus was similar to the previous compromise proposal of the Latvian Presidency. The "Option 2" set out in that document, in principle, followed the former Austrian/German proposal, specifying that the handling EDP shall obtain the necessary judicial authorisation in accordance with the law of that Member State (paragraph 2 of that proposal). Avoiding the term "recognition", Option 2 then specified that the assisting EDP shall, where required, obtain the necessary judicial authorisation; the court/judge in that Member State shall not, however, review the grounds, justification, and substantive reasons for ordering the measure. Thus, Option 2 was similar to what the Commission now claims to be the correct interpretation of Art. 31 EPPO Reg. This option, however, also did not (!) find the Council's approval. Instead, the Council eventually agreed on a concept for Art. 31, which, in principle, follows the draft text presented by the Latvian Presidency in June 2015.

Considering this background, it is hardly possible to reconcile the views expressed by the Commission in the present case on the correct interpretation of Art. 31 with the apparent intentions of the Union legislator.

### 3. Protection of fundamental rights – "more than mutual recognition"

AG *Ćapeta* also considered it appropriate to address the views expressed by Austria and Germany that the court in the assisting EDP's Member State needs to be able to undertake a full judicial review, as this is necessary in order to ensure effective protection of fundamental rights. Furthermore, she refers to the fact that proponents of Option Two had argued that Art. 31 does not provide for a system of mutual recognition but "something more." She then explains why she does not agree with that view: "as long as there are no common EU criminal law rules, the EPPO cannot but operate based on mutual recognition." In her view, "the levels of mutual recognition differ, and the EPPO may be seen as the most developed mutual recognition instrument in the area of cooperation in criminal matters yet." (mn. 78). This then leads her to detailed reflections on the nature of mutual recognition in criminal matters, in general, and in the EIO Directive, in particular. Comparing these solutions with the EPPO Regulation, she concludes that "[t]he EPPO is a single body and the assigned cross-border measures indeed need not be recognised, but only implemented." (mn. 101).

This reasoning is followed by her analysis of fundamental rights guarantees in the EPPO Regulation. She refers to the fact that the Commission had rightly pointed out that the EPPO Regulation does not contain grounds for non-recognition. She refers to Art. 31(5), which – instead – relies on an internal dialogue between the handling and the assisting EDPs. AG *Ćapeta* concludes that "[t]his internal cooperation system is one of the important elements for ensuring the protection of fundamental rights in the EPPO system." (mn. 105). She also admits, however, that "the EPPO cannot be assumed to be flawless." (mn. 108). But, in her view, the EPPO Regulation contains sufficient additional mechanisms. In this respect, she refers to the provisions in Art. 41 on procedural rights and in Art. 42 on (subsequent) judicial review.

Finally, AG *Ćapeta* recognizes that, for some Member States, this may lead to a decrease in the previously protected level of individual rights, and she concludes (mn. 113 f.):

> "[h]armonisation, after all, inevitably leads to a weakening of the protection of fundamental rights in Member States with a higher prior level of protection, unless the highest standard is adopted as a common rule. That, however, is the price of building a future together."

This conclusion is rather surprising in the present context: The "procedural rights directives" referred to in Art. 41(2) EPPO Reg. guarantee only a minimum level of protection, and they have not been specifically attuned to the new challenges for the defence posed by the EPPO.[17] While the Commission's proposal for the EPPO Regulation contained some additional specific provisions on procedural rights[18] as well as a catalogue of investigation measures in respect of which Member States would have been required to provide for an *ex ante* judicial authorisation,[19] the majority of Member States in the Council did not agree to any such harmonisation attempts but simply wanted to have national law apply. It remains to be seen whether the assumption of the Advocate General is correct that Art. 42(1) EPPO Reg. actually "requires that judicial review of investigation measures is always available" (mn. 112).[20] Perhaps this will soon be for the ECJ to decide.

## V. Consequences of the Solution Proposed by AG *Ćapeta* and Own Conclusion

Considering the numerous questions that arise in respect of the literal and contextual interpretation advocated by the Commission and the other proponents of "Option Two" as well as the difficulties to reconcile that solution with the legislative history of the EPPO Regulation, the question remains: Should one nevertheless follow the proposed conclusions by the Advocate General, as "preference must be given to that interpretation which ensures that the provision retains its effectiveness." (mn. 65)?

Obviously, the EPPO needs to be able to apply workable provisions on cross-border investigations. And it was to be expected that Art. 31 EPPO Reg. may lead to difficulties in this respect. Perhaps the ECJ will find a way to apply to its provisions an interpretation that at least solves the most immanent issues for the EPPO. In any case, however, the legislator would still be called upon to speedily amend the provisions of Art. 31: If the Court follows the Advocate General's proposal, the Union legislator should clarify the text and bring it in line with its presumed intention to establish an efficient system of cross-border investigations. Also, the legislator would need to clarify a number of open questions (see IV.2. a) and b) above). In addition, national legislation in Austria and Germany and perhaps in other Member States whose national legislators had faithfully relied on the assumption that Art. 31 actually means what it says, may have to be amended. Alternatively, if the Court follows the interpretation given by the proponents of "Option One", the EU legislator should amend Art. 31 in order to ensure that it does indeed provide rules for an efficient system of cross-border investigations.

Would the Advocate General's solution regarding the correct interpretation of Art. 31 be a suitable system of rules on cross-border investigation? A solution whereby a required judicial authorisation in terms of legality and sub-

stantial grounds is to be obtained from a court/judge in the Member State of the handling EDP would certainly make life easier for the EPPO and the courts, as there would normally be no need to call upon a court in the assisting EDP's Member State to undertake a substantial *ex ante* review of the ordered measure. It should normally also make it easier for the defence to estimate its legality and appropriateness and, where necessary, to challenge such a judicial authorisation or court order/warrant in the Member State in which the investigation is being conducted. Moreover, a judicial authorisation in the Member State of the handling EDP may also better ensure that the evidence gathered on this basis can indeed be used as such in the main criminal proceedings.

If one wishes to achieve that solution by interpreting the present text of Art. 31(2), as proposed by the Commission and other proponents of "Option Two", to also address the judicial authorisation of the ordered measure, the decisive question is: What purpose/meaning then remains for paragraph 3 of Art. 31? Neither the wording and context nor the EPPO's legislative history offer a satisfactory answer. If the Court nevertheless follows the view, also shared by the Advocate General, that paragraph 3 concerns only the "judicial authorisation of the enforcement" of the ordered measure, the question remains as to what exactly the scope and frame of reference for such a judicial authorisation could be. The text of Art. 31 does not provide an answer to this. As may be seen by looking at the legislative history, the Council did not have any intention of limiting the scope of the *ex ante* judicial review by the courts in the Member State of the assisting EDP. This is why Art. 31 does not contain any rules in this respect and why subparagraph 2 of Art. 31(3) merely contains a rule on the consequences of a decision by the court/judge in the assisting EDP's Member State not to grant judicial authorisation of the "assigned" measure. The text of Art. 31 neither contains any indication that it was the legislator's intention to stipulate that "assigned cross-border measures indeed need not be recognised, but only implemented" nor would it be appropriate to insert such a clause by way of interpretation of its provisions, as suggested by the Advocate General (mn. 101). And in case of investigation measures that require judicial authorization, it would not be appropriate to replace the judicial authorisation in the assisting EDP's Member State simply by a system of "consultation" between the involved EDPs, as AG *Ćapeta* suggests (mn. 105).

In the absence of any clarification that may be provided by the Union legislator, paragraph 3 of Art. 31, if interpreted by the Court to refer to the "judicial authorisation of the enforcement" of the assigned measure, should thus be seen as a provision on "recognition" of the assigned measure by a court/judge in the Member State of the assisting EDP – in analogy to the provision on "recognition and execution" in Art. 9(1) of the EIO Directive. This recognition may be refused (cf. subparagraph 2 of Art. 31(3)), and it will eventually be up to the legislator to clarify which "grounds for refusal" may be applied. The court in the assisting EDP's Member State should, however, take into account whether a court in the handling EDP's Member State already reviewed the admissibility of the measure and should refrain from undertaking its own substantial review in terms of grounds and appropriateness. Furthermore, the Union legislator could in this respect aim at a solution that it may consider to be an improvement over the EIO Directive: limiting the grounds for refusal, perhaps along the lines set out in Art. 31(5), which apply in case of investigation measures that do not require a judicial authorisation. Whether – in the current absence of any provision to that effect – such a limitation of the "grounds", also in case of a required judicial authorisation, may be "read" into Art. 31 by way of interpretation of its provisions is – again – a difficult question. But the ECJ may find a viable solution in this regard, as well.

1 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), *O.J.* L 283, 31.10.2017, 1.

2 H.-H. Herrnfeld, in H.-H. Herrnfeld/D. Brodowski/C. Burchard, *European Public Prosecutor's Office, Article-by-Article Commentary*, Baden-Baden 2021, Art. 31 mn. 4 et seq., 38 et seq.

3 *Herrnfeld*, ibid. Art. 31 mn. 4.

4 Cf. College Decision 006/2022 of 26 January 2022 adopting guidelines of the College of the EPPO on the application of Article 31 of Regulation (EU) 2017/1939; also available at <https://eppo-lex.eu/cdn_01/> accessed 17 July 2023.

5 Opinion of Advocate General *Tamara Ćapeta* delivered on 22 June 2023 in Case C-281/22, *G.K., B.O.D. GmbH, S.L.*, ECLI:EU:C:2023:510.

6 Section 3(2) of the German EUStAG – Act of 10 July 2020 to implement the EU Regulation establishing the European Public Prosecutor's Office, BGBl. I, p. 1648; an English translation has been published on <https://eppo-lex.eu/eppo-atlas-germany/>. In a similar vein: Art. 11(1) of the Austrian implementing law; an English translation has been published on <https://eppo-lex.eu/eppo-atlas-austria/> accessed 17 July 2023.

7 References to the margin numbers of the Advocate General's Opinion, *op. cit.* n. (5).

8 Here, AG *Ćapeta* refers, by way of example, to the judgment of the ECJ in case C-434/97, *Commission vs. France*, ECLI:EU:C:2000:98, mn. 21.

9 Cf. judgement of the ECJ of 8 June 2023 in Joined Cases C-430/22 and C-468/22, *VB and VB*, ECLI:EU:C:2023:458, mn. 24 with further references.

10 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *O.J.*, L 130, 1.5.2014, 1.
11 *Herrnfeld*, in Herrnfeld/Brodowski/Burchard, *op. cit.* n. (2), Art. 31 mn. 5, 38.
12 Cf. in particular the formal declaration of the Austrian delegation of 8 October 2015, addressed to the Council, DS 1547/15.
13 See Art. 26(4) of the Commission's Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, COM(2013) 534 final.
14 Council document DS 1237/15 of 21 April 2015.
15 Council document 9372/15 of 12 June 2015.
16 Council document 11045/15 of 31 July 2015.
17 *D. Brodowski*, in Herrnfeld/Brodowski/Burchard, *op. cit.* n. (2), Art. 41 mn. 63 with further references; for a detailed analysis see also: *V. Costa Ramos*, "The EPPO and the equality of arms between the prosecutor and the defence", (2023) 14(1) *New Journal of European Criminal Law*, 43 et seq.
18 Art. 33 to 35 of the Commission proposal, *op. cit.* n. (13)
19 Art. 26(4) of the Commission proposal, *op. cit.* n. (13)
20 See on this question: *Herrnfeld,* in Herrnfeld/Brodowski/Burchard, *op. cit.* n. (2), Art. 42 mn. 31 et seq.

**Dr. Hans-Holger Herrnfeld**
Senior Federal Prosecutor (Germany) – retired; former Head of Division at the German Federal Ministry of Justice

# Remote Biometric Identification and Emotion Recognition in the Context of Law Enforcement

## From the AI Regulation Proposed by the Commission to the EU Co-Legislators' Positions

Evangelos Zarkadoulas and Vagelis Papakonstantinou

**In April 2021, the European Commission put forward a proposal for a Regulation to harmonise rules on artificial intelligence (AI) across the EU, including AI in the context of law enforcement. Its horizontal character raised concerns in the police community, prompting a response by some Member States arguing for a separate legal act on the use of AI by law enforcement agencies. Two controversial components that have drawn the attention of the Council of the EU and the European Parliament are remote biometric identification and emotion recognition technologies. While the Council's general approach aligns with the Commission's proposal to balance law enforcement and human rights protection, the European Parliament pursues a narrower approach, advocating for the prohibition of real-time remote biometric recognition and emotion inference applications. It goes without saying that the outcome of the ongoing inter-institutional negotiations (trilogue) between the EU co-legislators and the Commission is being anticipated by law enforcement bodies with considerable interest. After all, this will define how the opportunities provided by AI are leveraged in law enforcement settings as well as how to deal with the misuse of this evolving technology by terrorists and criminals. This article reports on the institutions' positions on remote biometric identification and emotion recognition and highlights the – in the authors' view – flawed approach by the European Parliament toward law enforcement.**

### I. Introduction

Recently, artificial intelligence (AI) has been a top-agenda item worldwide. Rapid and ongoing technological advances in AI have triggered legislative initiatives to regulate its use in Europe. In April 2021, the European Commission tabled a proposal for a Regulation laying down harmonised rules on artificial intelligence across the EU.[1] It is based on Art. 114 of the Treaty on the Functioning of the European Union (TFEU), conferring upon the EU competence for the single market, in conjunction with Art. 16 TFEU, providing for legislation on the protection of individuals in the context of the processing of their data. Consequently, this proposal is a horizontal legislative act addressing the function of the internal market whilst also covering the field of law enforcement. A key feature of this proposal is that the Commission has adopted a risk-based approach for classifying AI applications into four categories: prohibited

practices, high risk with robust requirements, medium-low risk with transparency obligations, and minimal-no risk without rules.[2]

Law enforcement has been mainly classified under high-risk systems. This decision by the Commission raised concerns in the police community. At the Justice and Home Affairs Council in June 2021, some Member States suggested that a separate legal text on the use of AI by law enforcement authorities be adopted.[3] Their arguments related to the special nature of the police sector and the method followed in setting up the EU personal data protection framework consisting of the General Data Protection Regulation (GDPR) and the Directive 2016/680 (the Law Enforcement Directive). Undoubtedly, the monopoly on legitimate violence distinguishes law enforcement authorities from the remainder of public administration, as the former are responsible for public security and contribute to national security in the field of counter terrorism. What is more, discipline and implementation of criminal law are fundamental elements of the police remit. However, due to the limited support by other Member State delegations in the Council, the Commission's proposal was ultimately backed in its original wording.

The following sections provide an overview of the institutions' positions on remote biometric identification and emotion recognition tools. First and foremost, the article presents the relevant provisions of the Commission's proposal (Section II.). Subsequently, Sections III. and IV. outline the opinions of the Council of the EU and the European Parliament, and how these differ. In conclusion, the article highlights how the Commission and the Council have been able to strike a balance between law enforcement needs and fundamental rights – unlike the European Parliament, which has adopted a problematic angle when it comes to law enforcement.

## II. Remote Biometric Identification and Emotion Recognition AI Systems in the Commission Proposal

Two of the Regulation's components that have attracted significant attention during the discussions in the European Parliament and the Council are remote biometric identification and emotion recognition. The Commission has proposed categorising real-time remote biometric identification in public spaces for law enforcement purposes as a prohibited practice unless substantive and procedural prerequisites apply (Art. 5 of the proposal). With regard to these substantive requirements, the Commission has proposed that the use of this technology must pursue one of the following objectives: a) search for potential crime victims, for example, missing minors; b) prevention of threats to the life and physical safety of individuals or a terrorist incident; or c) detection, identification, or prosecution of a perpetrator or a suspect of a criminal offence referred to in Art. 2(2) Council Framework Decision on the European Arrest Warrant, and punishable with at least three years of a custodial sentence or a detention order under the rules of the Member State concerned. In terms of national procedures, prior authorisation by a judicial or an independent administrative authority is deemed necessary. Nevertheless, the proposal also provides for such authorisation being sought during an operation or ex-post in case of emergency.

Notwithstanding that Art. 5 of the Commission proposal allows real-time at a distance biometric recognition, Annex III defines it as a high-risk AI tool, and the conditions set out for high-risk AI applications must be met. In particular, these requirements include a risk management system, data governance, technical documentation, record-keeping, transparency, human oversight and accuracy, robustness, and cybersecurity (Arts. 8-15 of the proposal).

Annex III also classifies post biometric identification and emotional inference for law enforcement as high-risk. Consequently, this means that law enforcement will need to adhere to the requirements listed above if it intends to harness these tools.

In contrast, the Commission proposal sees the private sector exploiting these technologies more flexibly. It is noteworthy in this context that Art. 5 of the Commission proposal stipulates no requirements for real-time biometric identification in the non-public sector, while Art. 52(2) defines that emotion detection is considered a medium-low risk application with only transparency obligations.[4] This raises the question of why the Commission appears to trust private companies more than law enforcement authorities.

Moreover, when the College of Commissioners approved the legislative proposal on AI, the European Data Protection Supervisor (EDPS) asked for a moratorium on implementing remote biometric identification.[5] In particular, the EDPS – in collaboration with the European Data Protection Board (EDPB) – recommended a ban on the automated recognition of human biometric features in publicly accessible spaces through a joint opinion circulated in June 2021.[6] Despite these recommendations by the EDPS and the EDPB, the Commission has not amended its view, insisting on its initial proposal.

## III. The Council's General Approach

Following long internal consultations by the Member State delegations in the Working Party on Telecommunications and Information Society, the Member States endorsed their common position at the Transport, Telecommunications, and Energy Council in December 2022.[7] In view of the remarkable margin of action granted to the private sector when implementing remote biometric identification and emotion recognition in the Commission proposal (see Section II.), the Council has proposed revising the definition of law enforcement in Art. 3(41) and added all other entities that operate on behalf of law enforcement authorities. As for real-time remote biometric identification and emotion recognition, this addition has been incorporated in Art. 5, par. 1(d) and Annex III, par. 6(b) respectively. As a consequence, these entities must respect the requirements stipulated by both Art. 5 on real-time biometric identification and Art. 8–15 on high-risk systems for both technologies.

Considering the definition of law enforcement authority as provided for in Art. 3(40)(b) of the Commission proposal, the objective of this addendum is to include non-state actors not authorised by Member State legislation to perform law enforcement duties. Moreover, the Council has amended the scope of biometric identification by extending it to other offences apart from those listed in Art. 2(2) of the Framework Decision on the European Arrest Warrant, i.e. to include offences punishable by at least five years, as determined by national criminal law.

In relation to emotion recognition, the Council has clarified that affected individuals should not be informed in case of detection, prevention, and investigation of crime, thus defining more exceptions to the transparency obligation as proposed by the Commission in Art. 52 of the proposal. The reason for this amendment is that a person involved in a criminal activity may attempt to evade justice or adapt his or her behaviour when informed of being subject to emotion recognition, and thus render this technology ineffective. Likewise, EU and national criminal legislation stipulate criteria under which a suspect or a defendant needs to be informed of actions performed by the police and judicial authorities in order not to jeopardise an ongoing investigation.

## IV. The Parliamentary Position

Following the Council's general approach, the report on the AI Act was approved by the EP's Committees on Internal Market and Consumer Protection (IMCO) and on Civil Liberties, Justice and Home Affairs (LIBE) in May 2023,[8] before the EP's plenary adopted the position in June 2023.[9] From the Parliament's perspective, real-time and post remote biometric identification of natural persons, as well as emotional inference, are to be considered prohibited practices. In particular, real-time remote biometric recognition and emotion detection would be banned, even in the context of combating crime.

Yet, retrospective biometric identification is held permissible for law enforcement if the following prerequisites apply: a) *ex-ante* permission by a judicial authority; b) targeted search; and c) link with the investigation of committed serious crimes listed in Art. 83(1)TFEU (terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime, and organised crime).

Nonetheless, the proposed requirement of prior judicial authorisation for post-event biometric recognition applications might have an adverse effect on arresting criminals. Time is a critical factor in criminal investigations in progress, and the obligation to seek judicial permission could, for instance, enable a perpetrator to escape or obstruct the prevention of a terrorist attack or an offence against life.

## V. Conclusion

When it comes to the use of remote biometric identification and emotional inference systems in law enforcement, the Council largely agrees with the Commission's AI Act proposal. Its position does not meaningfully deviate from the Commission's proposal aimed at reconciling law enforcement and human rights protection. On one hand, police authorities are to be enabled to better leverage technology to tackle terrorists and criminals who exploit state-of-the-art technology without running into legal restrictions; on the other hand, the principle of proportionality and fundamental rights are to be respected. As a result, both institutions render real-time remote biometric recognition admissible by stipulating substantive and procedural criteria under which law enforcement bodies need to comply.

In contrast, the European Parliament's position reveals a stricter approach, considerably restricting the implementation of AI by the police. From an operational perspective, a major impact of this stance would be the prohibition of AI biometric systems to prevent terrorism and crime. Law enforcement agencies would not be able to use remote biometric identification and emotion recognition to deter terrorist attacks and crimes, ensuring public security, and protecting

individuals from victimisation. One additional consequence would be the inability of the police to apply remote biometric identification to detect missing persons and, notably, minors. As regards post remote biometric identification of natural persons, which is a long-standing successful forensic tool, prior judicial authorisation as proposed by the EP will likely harm the swift analysis of recorded footage and – ultimately – the effectiveness of criminal investigations.

Inevitably, the ongoing inter-institutional negotiations (trilogue) between the EP and the Council as EU co-legislators and the Commission are complicated, and a compromise agreement will be hard to achieve. In any case, law enforcement authorities expect the outcome of the negotiations with great interest because this will define how the opportunities offered by AI can be leveraged as well as how to tackle the misuse of this emerging technology by criminals.

1 European Commission, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts", COM(2021) 206 final.
2 European Commission, Press Release, "Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence", <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682> All internet links referred to in this article were last accessed on 5 October 2023.
3 One of the authors (Evangelos Zarkadoulas) personally attended this Council meeting; for the main results, see Council of the EU, Justice and Home Affairs Council, 7–8 June 2021, <https://www.consilium.europa.eu/en/meetings/jha/2021/06/07-08/>.
4 Apart from emotion recognition, this provision governs the biometric categorisation systems, which aim to classify natural persons into specific categories, and not to identify them in the way biometric identification tools do.
5 EDPS, Press Release, "Artificial Intelligence Act: a welcomed initiative, but a ban on remote biometric identification in public space is necessary", <https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en>.
6 EDPB-EDPS, "Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)", <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf>.
7 Council of the EU, Transport, Telecommunications and Energy Council (Telecommunications), 6 December 2022, Main results, <https://www.consilium.europa.eu/en/meetings/tte/2022/12/06/>.

**Evangelos Zarkadoulas, Ph.D. Law Student**
Vrije Universiteit Brussels (VUB), Faculty of Law and Criminology

**Prof. Vagelis Papakonstantinou**
Professor on Personal Data Protection Law, Vrije Universiteit Brussels (VUB), Faculty of Law and Criminology

8 European Parliament, Press Release, "AI Act: a step closer to first rules on Artificial Intelligence", <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence>.
9 European Parliament, Press Release, "MEPs ready to negotiate first-ever rules for safe and transparent AI", <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai>.

# Imprint

## Impressum

Published by:
**Max Planck Society for the Advancement of Science**
**c/o Max Planck Institute for the Study of Crime, Security and Law**
(formerly Max Planck Institute for Foreign and International Criminal Law), represented by Director Prof. Dr. Ralf Poscher
Guenterstalstrasse 73
79100 Freiburg i.Br., Germany

Tel: +49 (0)761 7081-0
E-mail: public-law@csl.mpg.de

Internet: https://csl.mpg.de

Official Registration Number: VR 13378 Nz
(Amtsgericht Berlin Charlottenburg)
VAT Number: DE 129517720

Editor in Chief: Prof. Dr. Dr. h.c. mult. Ulrich Sieber
Managing Editor: Thomas Wahl, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Editors: Dr. András Csúri, Vienna University of Economics and Business; Dr. Anna Pingen, Max Planck Institute for the Study of Crime, Security and Law, Freiburg; Cornelia Riehle, ERA, Trier
Editorial Board: Prof. Dr. Lorena Bachmaier, Complutense University Madrid, Spain; Peter Csonka, Head of Unit, DG Justice and Consumers, European Commission Belgium; Prof. Dr. Esther Herlin-Karnell, University of Gothenburg, Sweden; Mirjana Juric, Head of Service for combating irregularities and fraud, Ministry of Finance, Croatia; Philippe de Koster, Director FIU Belgium; Prof. Dr. Katalin Ligeti, University of Luxembourg; Dr. Lothar Kuhl, Head of Unit, DG REGIO, European Commission, Belgium; Prof. Dr. Ralf Poscher, Director at the Max Planck Institute for the Study of Crime, Security and Law, Freiburg, Germany; Lorenzo Salazar, Deputy Prosecutor General to the Court of Appeal of Naples, Italy; Prof. Rosaria Sicurella, University of Catania, Italy
Language Consultant: Indira Tie, Certified Translator, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Typeset: Katharina John, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Produced in Cooperation with: Vereinigung für Europäisches Strafrecht e.V. (represented by Prof. Dr. Dr. h.c. mult. Ulrich Sieber)
Layout: Ines Hofmann, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Printed by: Stückle Druck und Verlag, Ettenheim, Germany

**The publication is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF)**

Co-funded by the European Union


ISSN: 1862-6947

### Practical Information

Articles in eucrim are subject to an editorial review. The journal is published four times per year and distributed electronically for free.
In order to receive issues of the periodical on a regular basis, please write an e-mail to:
eucrim-subscribe@csl.mpg.de.
For cancellations of the subscription, please write an e-mail to:
eucrim-unsubscribe@csl.mpg.de.

More information at our website: https://eucrim.eu

### Contact

Thomas Wahl
Max Planck Institute for the Study of Crime, Security and Law
Guenterstalstrasse 73
79100 Freiburg i.Br., Germany
Tel: +49(0)761-7081-256 or +49(0)761-7081-0 (central unit)
E-mail: info@eucrim.eu

https://eucrim.eu/

MAX PLANCK INSTITUTE
FOR THE STUDY OF
CRIME, SECURITY AND LAW