eucrim 2025 / 4
European Law Forum: Prevention • Investigation • Prosecution

Surveillance
Surveillance
Überwachung

2025 / 4 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

Articles

Editorial

Dear Readers,

This *eucrim* issue provides insights into various aspects of state surveillance, a subject that has long engaged both the public and the legal community. Rapid technological advances, political initiatives, and landmark rulings by the highest national and European courts have fueled this interest. Digitalisation and the (seemingly) boundless potential of artificial intelligence provide new opportunities for data mining and analysis that can be (mis-)used for the surveillance of citizens, with potentially unprecedented consequences for those targeted. Prominent examples of the potential impact of contemporary surveillance practices, based on the retrieval, transfer, and processing of personal data through forensic analyses, are the recent landmark police operations targeting encrypted phone providers like EncroChat, SkyECC, and ANOM, which are also highlighted in this issue. For some, these cases serve to underline the promise of new technologies, while for others they exemplify the risks of pervasive surveillance.

In the past, discourse on surveillance has mostly centered on the powers of law enforcement and intelligence agencies. Less attention has been paid to surveillance carried out by police and other security agencies in the course of their preventive agendas, even though the boundary between preventive and repressive police activities has become increasingly fluid. In principle, any untargeted police observation and activity on the streets may find its way into a prosecutorial or court file. Moreover, the transnational dimension of data sharing is of growing significance.

Apart from the spectacular and sometimes pioneering cases that attract the most attention, little is known about the day-to-day routines of security agencies. These practices can affect communications, online activities and interpersonal interactions on social media, daily commuting by car and occasional air travel, ordinary and extraordinary financial activities, and anything stored on a local computer or in the cloud. In short, people's entire digital lives can easily be traced and retrieved by public agencies.

New opportunities give rise to new fundamental-rights questions. The sheer volume of digitalized data available to state agencies, whether for preventative or repressive purposes, requires a re-calibration of traditional proportionality models and new methods to determine the impact of digital, data-based surveillance activities. This impact must be assessed according to the severity of the related human-rights infringements. From this perspective, proportionality calibrated to severity has both qualitative and quantitative dimensions. One such assessment model is the Surveillance Barometer developed in my department at the Max Planck Institute for the Study of Crime, Security and Law. Designed as a theoretically and empirically grounded instrument, it measures and assesses the current state of surveillance and the associated burdens from a citizen's perspective in Germany.

Ralf Poscher

A crucial issue we identified is the need for state agencies to be transparent about their activities. Reliable statistical data on the types and numbers of surveillance measures actually carried out is often lacking. This lacuna on the part of state actors can intensify public concern based on misguided assumptions. As Kilchling and Ellebrecht rightly point out in their article outlining the Surveillance Barometer project, the popular discursive picture of excessive surveillance of citizens may be considered a symptom of deficiencies in transparency.

I hope that transparency will improve in more areas in the future, including surveillance powers and their application from national and supranational perspectives. A good starting point is Union legislation requiring Member States to provide meaningful statistical data on the implementation of Union-law-based activities on a regular basis.

Prof. Dr. Ralf Poscher, Director at the Max Planck Institute for the Study of Crime, Security and Law, Public Law Department, Freiburg

News

Actualités / Kurzmeldungen

European Union

Reported by Thomas Wahl (TW), Cornelia Riehle (CR), Dr. Anna Pingen (AP)

Foundations

Fundamental Rights

25 Years of Charter of Fundamental Rights

spot light

On 7 December 2025, the EU celebrated the 25th anniversary of the Charter of Fundamental Rights of the European Union ("the Charter" or CFR in short). On 7 December 2000, EU leaders solemnly proclaimed the Charter in Nice, France. At that time, the Charter had no legally binding effect. However, it carried political significance and the CJEU regularly referenced Charter rights in its case law in subsequent years. When the Lisbon Treaty came into force on 1 December 2009, the Charter was given "the same legal value as the Treaties" (Art. 6(1) TEU). This means the rights enshrined in the Charter are legally binding on EU institutions and EU countries when they implement EU law. Its 50 fundamental rights and freedoms, which are grouped under six titles, establish a common basis of principles and values that guarantee protection for the essential rights of all European Union citizens. The Charter has become the "cornerstone" of the EU's legal system.

To celebrate the 25th anniversary, the European Commission, the European Agency for Fundamental Rights (FRA) and the Danish Council Presidency jointly organised a conference in Brussels on 10–11 December 2025. Under the title "25 Years of Rights: Reflecting on the Impact of the Charter", participants also discussed the future of the Charter and how to raise awareness of the Charter's relevance in daily life further. In this context, the Commission published the results of a special Eurobarometer survey, which found that 49% of European respondents said they were aware of the Charter while 51% of respondents said they had not heard of it. And even 80% of respondents said that they do not feel well informed about the Charter.

To mark the anniversary, the Commission has published a series of videos featuring people from across the EU reflecting on how fundamental rights matter in daily life. The Commission also emphasised its efforts to strengthen the application of the Charter within the EU. These efforts include the 2020 "Charter Strategy", which sets out the direction for the Charter's implementation until 2030 (→eucrim 4/2020, 259–260) and the annual reports, which monitor the progress on the application of the Charter (→eucrim 4/2023, 306–307). The 2025 annual report, published on 5 December 2025, reviewed progress halfway through the 2020 Strategy. It concluded that determined action is needed to strengthen the respect for, and protection of, the Charter's rights across all EU policy areas. For the second half of the Strategy's implementation (2026–2030), the Commission will engage in further policy measures and support deeper cooperation among EU institutions, Member States, and other stakeholders.

Another important pillar for assistance and expertise on the application of the Charter in the EU institutions and EU Member States are the EU Agency for Fundamental Rights (FRA) and the European Institute for Gender Equality (EIGE). The FRA, *inter alia*, provides annual fundamental rights reports, which give an overview of the state of fundamental rights in the EU and highlight critical developments and trends in a year. The FRA also runs Charterpedia that informs in a practical way and as a single source about the fundamental rights that people have under EU law. (TW)

* Unless stated otherwise, the news items in the following sections cover the period 16 November 2025 – 15 January 2026. Have a look at the eucrim website (https://eucrim.eu), too, where all news items have been published beforehand.

EU JHA Heads Strengthen Fundamental Rights Compliance

From 4 to 5 December 2025, the Heads of EU Justice and Home Affairs (JHA) Agencies met in Vienna to review joint achievements and align future cooperation with broader EU priorities.

The meeting brought together the Heads of the EU JHA Agencies (e.g., CEPOL, Europol, Eurojust, Frontex, eu-LISA, FRA, etc.) and representatives from the European Parliament; the Danish and Cypriot Council Presidencies; the Danish coordinator of the European Multidisciplinary Platform Against Criminal Threats (EMPACT); the European Commission; the European External Action Service; and the EU Agencies Network.

Key topics discussed included the EU Internal Security Strategy ProtectEU (→eucrim 1/2025, 3–4), the EU Innovation Hub for Internal Security, and the AI Act (→eucrim 2/2024, 92–93).

To mark the 25th anniversary of the EU Charter of Fundamental Rights (→previous news item), the Heads of the JHA Agencies also adopted a joint statement expressing their commitment to strengthening the protection and promotion of fundamental rights and compliance with the Charter across all agency activities. Furthermore, they published a consolidated overview on the measures taken since 2019 to embed Charter compliance in the activities of each JHA Agency.

A central theme is the institutionalisation of fundamental rights oversight. Agencies with significant operational mandates, such as Europol, Frontex, and the EU Agency for Asylum (EUAA), have strengthened the role of independent Fundamental Rights Officers (FROs), supported by monitoring mechanisms, complaints procedures, and binding codes of conduct. For Frontex, this includes the deployment of Fundamental Rights Monitors in the field and expanded safeguards in return operations. The EUAA has adopted a Fundamental Rights Strategy (2024–2028) and enhanced its complaints mechanism for individuals affected by asylum support operations.

Training and capacity-building are key compliance tools. CEPOL has fully mainstreamed fundamental rights and data protection across law enforcement training curricula, treating them as cross-cutting requirements rather than standalone topics. FRA, Europol, and Frontex contribute substantively to joint training initiatives, particularly on policing standards, vulnerable groups, hate crime, data protection, and asylum procedures. Notably, the FRA continues to target judges and legal practitioners through Charter-specific tools.

From a data protection and digital governance perspective, eu-LISA and the EU Drugs Agency (EUDA) play a prominent role. eu-LISA, responsible for large-scale IT systems such as SIS, VIS, EURODAC and the newly launched Entry-Exit System (EES), frames data protection and freedom of movement as core Charter obligations embedded throughout system design and operation. Interoperability, data protection by design, and cooperation with the European Data Protection Supervisor feature prominently. EUDA highlights robust compliance with Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices, and agencies, including breach response policies, transparency registers, and internal audit structures.

For criminal justice practitioners, Eurojust highlights its role in safeguarding defence rights, *ne bis in idem*, victims' rights, and data protection in cross-border cooperation, notably in European Arrest Warrant proceedings and jurisdictional conflicts. Eurojust's strategic publications on CJEU case law are positioned as practical reference tools. Europol has strengthened its commitment to fundamental rights, data protection, and diversity & inclusion across its operations. Europol's FRO now oversees compliance, including involvement in research, innovation, and external relations, while advising management and monitoring potential rights violations. The 2022 Recast of the Europol Regulation further enhanced rights safeguards, parliamentary scrutiny, and the agency's ability to process complex operational data.

Overall, the report illustrates a shift from declaratory Charter commitments toward operationalisation, with measurable structures, accountability mechanisms, and inter-agency coordination. (CR)

Rule of Law

ECJ Reprimands Polish Constitutional Court and Denies its Independence

In the dispute over the primacy of EU law over national constitutional law and the decision-making powers of the highest courts, the Grand Chamber of the European Court of Justice (ECJ) has once again reaffirmed the ECJ's position: In its judgment of 18 December 2025 in infringement proceedings C-448/23 brought by the European Commission against Poland (→eucrim 1/2023, 4), the judges in Luxembourg postulate that national constitutional courts cannot override the primacy of EU law either by invoking their respective constitutional identity or by means of *ultra vires* review.

➤ *Background of the case*

The case was prompted by rulings of the Polish Constitutional Court on 14 July and 7 October 2021, which questioned the compatibility of EU law and the rulings of the ECJ with the Polish constitution (→eucrim 3/2021, 135 et seq.). The criticised ECJ rulings were issued in connection with the controversial judicial reform under the national-conservative PiS government.

In its ruling of 14 July 2021, the Polish Constitutional Court found that the interim measures imposed by the ECJ on the organisation of the courts (Case C-791/19 R (→eucrim 1/2020, 4)) violated the principle of specific conferment of powers and the Polish constitutional identity. In view of this alleged conflict of norms, the Polish Constitutional Court reaffirmed the primacy of the constitution as the supreme source of law in Poland. In its ruling of 7 October 2021, the Polish Constitutional Court declared unconstitutional certain provisions of EU law as interpreted by the ECJ (Cases C-824/18, *A.B. and Others* (→eucrim 1/2021, 4) and C-487/19, *W.Ż.* (→eucrim 3/2021, 136)), according to which national courts are empowered, among other things, to review the legality of the procedures for appointing judges.

The European Commission then initiated an action for failure to fulfil obligations against Poland, alleging violations of the principles of EU law, in particular the primacy of Union law and the binding effect of ECJ decisions. It also complained of serious irregularities in the appointment of three judges and the President of the Polish Constitutional Court, as a result of which the latter could no longer be regarded as an independent and impartial tribunal within the meaning of EU law.

➤ *The ECJ's ruling*

The ECJ upheld the complaint in its entirety. In its 2021 judgments, the Polish Constitutional Tribunal had violated the principle of effective judicial protection by denying the national courts the jurisdiction to review the legality of the procedures for appointing judges and to rule on the defective nature of these procedures, in disregard of the case law of the Court of Justice. It had also disregarded the binding effect of the interim measures issued by the Court of Justice concerning the organisation and jurisdiction of the Polish courts and the proceedings before those courts. In its reasoning, the ECJ also stressed the following issues:

- The judgments by the Polish Constitutional Court call into question the essential characteristics of the legal order of the European Union;
- After accession, Poland undertook legally binding obligations for the values enshrined in Art. 2 TEU (including the rule of law, effective judicial protection and the independence of the judiciary) and cannot escape from these obligations by relying on constitutional identity;
- National courts cannot unilaterally determine the scope and limits of the powers conferred on the Union.

Looking at the Commission's complaint involving specific appointments of judges to the Polish Constitutional Court, including its President, in 2015/2016, the ECJ concluded that these appointments were vitiated by infringements of fundamental rules relating to appointment procedures in Poland. As a consequence, the Polish Constitutional Court does not meet the requirements of an independent and impartial tribunal established by law, within the meaning of EU law and Poland has failed to fulfil its obligations under Art. 19(1) TEU.

➤ *Put in focus*

Beyond the specific dispute with the Polish Constitutional Court and the related judicial reform from 2015 onwards, which raises concerns about the rule of law, the ECJ ruling is another important landmark decision on the fundamental relationship between the law of Member States and EU law on the one hand, and – correspondingly – between national supreme courts or constitutional courts and the ECJ on the other. It reaffirms the primacy of EU law, which has been developed by the ECJ since the 1960s. With this ruling, the ECJ ultimately clarifies that the correct place to resolve discrepancies between national and European law is the preliminary ruling procedure under Art. 267 TFEU and no unilateral decision-making at the national court level.

It remains to be seen to what extent Poland itself will or can respond to the ruling. Under Art. 260(1) TFEU, Poland is obliged to take the necessary measures to comply with the ECJ's judgment. However, dismantling the judicial reforms implemented by the PiS government is proving extremely difficult for the liberal-conservative government led by Prime Minister Donald Tusk, which has been in office since December 2023 (→eucrim 1/2024, 4 and →eucrim 4/2024, 264–265). The Polish Constitutional Court, which was restructured by the then PiS government in the wake of the constitutional crisis at the end of 2015, is still largely in office in its former form at the beginning of 2026. In March 2024, however, the Sejm, the Polish parliament, denied the Constitutional Court's legitimacy, so that it is currently in a crisis of legitimacy because its decisions are being ignored. Conversely, the election of *Karol Nawrocki*, who is close to the PiS, as Polish President in June 2025 will continue to make judicial reforms in Poland difficult and protracted, as the President has the right to veto laws. It would certainly be contrary to the efforts of the new Polish government if the European Commission were to conclude that Poland had not responded adequately to the ruling from Luxembourg of 18 December 2025 and then, pursuant to Art. 260(2) TFEU, refer the matter back to the ECJ to request that a fine be imposed on Poland. (TW)

Area of Freedom, Security and Justice

Report of the High-Level Forum on the Future of EU Criminal Justice

spot light

On 1 December 2025, the High-Level Forum on the Future of EU Criminal Justice (HLF) published a final report summarising the discussions and key insights

from participants at the forum's plenary meetings.

Launched in February 2025, the HLF reviewed the progress made in the criminal limb of the Area of Freedom, Security and Justice and provided input for a new vision for the future of EU criminal justice. Organised by the European Commission and the Council Presidency, the Forum gathered more than 100 participants, including high-level representatives from the Member States, the European Parliament, relevant EU JHA bodies and agencies (OLAF, the EPPO, Europol, Eurojust, EJN, etc.). External stakeholders were also present, including representatives from academia, legal practitioners, defence lawyers' associations (ECBA, CCBE), civil society, and other organisations/networks. Throughout 2025, participants met in four plenary meetings to share their views on specific thematic issues involving the five main pillars of EU criminal justice:

- **Substantive criminal law,** focusing on the possible need to update the existing EU acquis;
- **Judicial cooperation** and mutual recognition in criminal matters, assessing the need to amend and clarify relevant EU instruments;
- **Procedural safeguards** in criminal proceedings, discussing how to strengthen procedural safeguards for suspects and accused persons, and address gaps in legislation;
- **Digitalisation** in criminal justice, reflecting on possible new non-legislative and legislative instruments, as well as the use and challenges of artificial intelligence (AI);
- **EU JHA agencies and bodies,** considering the future of Eurojust, Europol, the EPPO and OLAF in light of the envisaged review of their founding regulations.

The final report synthesises the key insights, priorities, and policy directions raised by participants during the meetings. As the views were sometimes contradictory, the report rather provides food for thought rather than clear recommendations. The report summarises the reflections made for each of the above-mentioned pillars in grey boxes. The main aspects for future direction can be outlined as follows:

➤ *Substantive criminal law*

- Focusing on the correct implementation of the existing EU acquis, and ensuring consistency and coherence among future criminal law legislative initiatives;
- Exploring possible adaptations to the existing EU substantive criminal law *acquis* in view of AI developments, including possible new EU legislation to tackle AI-enabled crime;
- Considering the need for, and adequacy of, legal bases for adopting new EU criminal law initiatives for maintaining respect for EU values, notably in the area of hate offences;
- Exploring the need to criminalise the violations of intellectual property rights, particularly the counterfeiting of medical products;
- Exploring the possible adoption of non-legislative measures to promote and support the Member States' action in crime prevention, including on the basis of Art. 84 TFEU.

➤ *Judicial cooperation and mutual recognition in criminal matters*

- Examining targeted amendments to the EIO Directive;
- Exploring rules on remote participation via videoconference in cross-border court hearings for suspects and accused persons;
- Considering ways to further strengthening the effectiveness of the functioning of the EAW, while focusing on non-legislative measures;
- Improving the coherence of the pre-Lisbon Framework Decisions via targeted amendments or non-legislative measures;
- Examining the opportunity to develop rules for cross-border investigations for the purpose of asset recovery in the execution phase;
- Pursuing the preparation of an Impact Assessment on the need for EU rules on data retention as a matter of legislative priority.

➤ *Procedural safeguards in criminal proceedings*

- Following-up on the measures taken by Member States in relation to the 2013 Recommendation on procedural safeguards for vulnerable persons (→eucrim 4/2013, 120–121);
- Effectively following-up on the 2022 Commission Recommendation on detention (→eucrim 4/2022, 250) and exploring further soft law measures on matters related to detention, or cross-border cooperation instruments on alternatives to detention, such as electronic monitoring;
- Exploring measures on the protection of legal professional privilege;
- Exploring non-binding actions on evidence gathering and admissibility of evidence in cross-border cases;
- Continuing to examine the need for further updates to the procedural rights *acquis* in light of new technological developments, including with respect to the recourse to AI-generated/produced evidence.

➤ *Digitalisation of criminal justice*

- Continuing to develop the general mapping exercise of the digitalisation of national justice systems and furthering EU funding for support with the digitalisation of justice through, *inter alia*, multi-country projects;
- Creating an IT toolbox (including AI tools) to help Member States accelerate their level of digitalisation and generate cost savings;
- Promoting the coordination of and the accessibility to national legislation and case-law online;
- Supporting the adoption of voluntary, non-binding common technical standards for videoconferencing and creating a videoconferencing hub to help overcome interoperability issues in cross-border videoconferencing;
- Examining the need for a legislative initiative to establish a criminal justice

cross-check mechanism to prevent *ne bis in idem* violations;

- Providing guidance on the use of high-risk AI systems in justice, emphasising that AI tools must remain strictly advisory and have robust human oversight.

➤ *EU JHA agencies and bodies*

- Reducing duplication of efforts and overlaps between JHA agencies and bodies;
- Considering the setting up of a modernised criminal justice cross-check mechanism involving JHA agencies and bodies, which would allow for multilateral (semi-)automated searches in each other's case management systems;
- Assessing the views expressed during the HLF in the context of the revisions to the Eurojust, Europol and EPPO Regulations;
- Further exploring the relevance and feasibility of extending the EPPO's competence to violations of Union restrictive measures.

➤ *Follow-up*

As an early step to put the discussions from the High-Level Forum into action, the European Commission published a consultation on the European Investigation Order (EIO) Directive 2014/41/EU on 6 January 2026. As discussed, the Directive is set to be ready for targeted amendments. Firstly, substantive and procedural additions to the EIO are to be examined. Secondly, the inconsistent legal situation in the Member States regarding the remote participation of suspects, accused persons and victims in court proceedings by video conference is to be addressed. By 3 February 2026, the Commission had received a total of 15 responses to the consultation. (TW)

Council Updates Model Provisions on EU Substantive Criminal Law

At its meeting on 8–9 December 2025, the Justice and Home Affairs Council approved Council conclusions on "Model provisions on EU substantive criminal law". The conclusions build on and update past conclusions on this matter, in particular: the 2002 conclusions "on the approach to apply regarding approximation of penalties"; the 2009 guidance for the Council's criminal law deliberations (→eucrim 4/2009, 140), and the 2024 conclusions on "the future of EU criminal law" (→eucrim 2/2024, 85–86).

The model provisions are designed to facilitate negotiations on horizontally applicable substantive criminal law provisions in EU instruments, such as inciting, aiding and abetting, penalties for natural and legal persons, aggravating/mitigating circumstances, jurisdiction, limitation periods, etc.

The Council stressed that the updated model provisions are not binding on the co-legislators, but constitute a toolbox that co-legislators can use for the formulation of repeating provisions that apply for all legislative acts harmonising crimes. The conclusions will guide the Council on any future legislative proposal in this regard, so that standard language ensures consistency, coherence and efficiency across EU legislation. (TW)

Commission Unveils Digital Justice Package 2030

On 20 November 2025, the European Commission presented its Digital Justice Package 2030, setting out a roadmap to modernise and digitalise justice systems across the European Union. The initiative aims to accelerate the use of digital tools and artificial intelligence (AI) in national courts and in judicial cooperation, with a view to improving efficiency, accessibility, and cross-border collaboration.

The package consists of two core components:

- DigitalJustice@2030 Strategy: 14 measures have been designed to promote the exchange of best practices and technological solutions. Among other steps, the Commission announced plans to facilitate the sharing of digital tools via the European e-Justice Portal, develop a common toolbox for IT and AI applications used in justice, and further expand the European Legal Data Space to improve access to legislation and case law. A study is also envisaged to explore technical solutions for interoperability challenges in cross-border judicial cooperation, including videoconferencing systems.
- European Judicial Training Strategy 2025–2030: The strategy focuses on equipping judges, prosecutors, court staff, and other legal practitioners with digital competences. It provides for practical training on digital case management, secure communication tools, and cross-border cooperation instruments as well as awareness-raising activities on the implications of AI in justice. It also emphasises the need for training on EU digital legislation, such as the Digital Services Act, and calls for stronger alignment between national and EU-funded training programmes.

The Commission framed the initiative as part of the EU's broader Digital Decade objectives and as a continuation of earlier efforts, including the 2023 Digitalisation Regulation (→eucrim 4/2023, 331–332), which enabled digital exchanges in a range of cross-border judicial procedures. The package was presented as a further step towards strengthening judicial systems through digital transformation and enhancement of their resilience and competitiveness. (AP)

Security Union

Statewatch: Campaign against Transnational Security Networks Needed

On 27 November 2025, Statewatch published the outcome of a research project that has examined how global counter-terrorism and security networks threaten civic space and human

rights. Entitled "Networks of (in)security", the project provides an evidence base showing how these security norms are implemented and identifying opportunities for change. The project's ultimate goal is to stimulate discussion and campaigns that advocate for increased democratic and public scrutiny and oversight of transnational security institutions. In the long term, an organised response should halt "the development of an unaccountable, invasive and harmful global security architecture."

The project outputs feature an overview of the research and analyses on thematic issues, including:

- Travel surveillance;
- Watchlists and watchlisting;
- Accountability and redress.

These are supplemented by country profiles.

According to Statewatch, increasing pre-emptive, automated and algorithmic forms of surveillance and profiling reinforce racism and discrimination, inhibit free movement, and give authoritarian states new tools of control. Several effects of the deployment of transnational security tools have been identified, including:

- The experimental nature of technologies and techniques, involving rules-based screening and network analysis tools, designed to assess the "risk" posed by indviduals and to map their social connections;
- The "transnational security project" is essentially characterised by the reconfiguration and reinforcement of state borders;
- International organisations and powerful states are spreading technologies and techniques of repression;
- Meaningful accountability and redress are substantially lacking.

The report concludes with a series of questions rather than recommendations. Statewatch encourages stakeholders and civil society to take these questions in order to scrutinise the global security alliance. (TW)

Schengen

Protecting Applicants' Rights Ahead of ETIAS Launch

As preparations continue for the launch of the European Travel Information and Authorisation System (ETIAS) in autumn 2026, the ETIAS Fundamental Rights Guidance Board (EFRGB) (→eucrim 2/2024) is playing a key role in ensuring compliance with data protection and other fundamental rights. The EFRGB is an independent advisory body that monitors fundamental rights compliance in ETIAS, provides recommendations to the ETIAS Screening Board, and advises on specific rights issues. Its members include representatives from Frontex, the EDPS, the EDPB, and FRA.

At the beginning of November 2025, the EDPS announced that the EFRGB had issued a new guidance note on how to ensure an applicant's right to an effective judicial remedy in the context of ETIAS. The guidance note clarifies the procedural obligations that apply when negative ETIAS decisions are taken – in line with Art. 47 of the EU Charter of Fundamental Rights and relevant CJEU case law. It also addresses key requirements, e.g., providing clear reasons for decisions, granting access to files, and ensuring transparency when decisions rely on sensitive data or algorithmic profiling. This guidance is now being examined by national authorities and EU agencies as they prepare ETIAS for entry into operation. (CR)

Ukraine Conflict

Europol and OLAF Crack Down on Sanctions Evasion

To step up its support to EU Member States combating sanctions evasion in conjunction with Russia's war of aggression against Ukraine, Europol has established a "Target Group Sanctions", a new team within its European Financial and Economic Crime Centre. Launched in November 2025, the target group aims to identify and disrupt criminal networks circumventing EU sanctions, leveraging Europol's intelligence, financial-tracing, and analytical capabilities.

In addition, Europol has teamed up with OLAF to launch "Project Transporter", which targets vehicle exports to third countries potentially destined for onward transfer to Russia and Belarus. This joint effort aims to counteract the increase in shipments enabled by forged documents and illicit financial practices. The project brings together specialists from EU Member States' customs, police, and financial crime services. The cooperation between Europol and OLAF reinforces the EU's collective response to sanctions circumvention. The project is part of EMPACT, the EU's instrument for structured multidisciplinary cooperation to fight serious international crime in line with pre-defined priorities. Customs fraud, including sanctions evasion, is one of EMPACT's priorities for the period 2026–2029 (→eucrim 2/2025, 142).

On 26 January 2026, OLAF reported on a concrete successful operation against vehicle transports to Russia. A coordinated law enforcement action revealed that over 760 vehicles originally destined for Turkey were actually moved to Russia. By carrying out extensive data analysis and cross-checking of customs, trade, and transport information, OLAF was able to reconstruct the transport chain, confirming the suspected circumvention of EU sanctions. The investigation led to criminal proceedings in three Member States. (CR/TW)

EU Reactions to Russian War against Ukraine: Overview End of November 2025 – February 2026

This news item continues the reporting on key EU/CoE reactions following the Russian invasion of Ukraine on 24 Feb-

ruary 2022: the impact on the protection of the EU's financial interests, on the EU's internal security policy, and on criminal law.

The following overview covers the period from November 2025 to February 2026. For overviews of developments in previous periods →eucrim 3/2024, 174–176, →eucrim 4/2024, 267–268, →eucrim 1/2025, 6–7 and →eucrim 2/2025, 114–118, each with further references.

■ **17–18 November 2025:** The European Anti-Fraud Office (OLAF) and Europol intensify their cooperation in order to address attempts to circumvent EU sanctions against Russia and Belarus. At a joint meeting, the two bodies examine emerging trends and discuss ways to improve coordinated enforcement. Member States report a significant increase in exports of vehicles to third countries, raising concerns that such exports may be used to bypass EU restrictive measures and indirectly support Russia's military capabilities. Investigations also reveal related criminal activities, including money laundering and document forgery. As part of their strengthened cooperation, OLAF and Europol launch a new operational initiative, "Project Transporter", aimed at supporting national investigations into possible breaches of sanctions. The initiative brings together investigators from customs, the police, and financial crime authorities to enhance coordination and share operational information in cases involving vehicle exports to Russia and Belarus (see also previous news item).

■ **20 November 2025:** The Council imposes restrictive measures on ten individuals responsible for serious human rights violations and for the repression of civil society and democratic opposition in Russia, including members of the Russian judiciary involved in the prosecution of journalists and human rights activists.

■ **3 December 2025:** The European Parliament and the Council reach a provisional agreement to permanently end Russian gas imports into the EU and gradually phase out Russian oil. The measures form part of the EU's REPowerEU strategy aimed at reducing dependence on Russian fossil fuels and strengthening Europe's energy security. The Commission will monitor implementation and may issue recommendations.

■ **3 December 2025:** The Commission presents a package of legal proposals aimed at addressing Ukraine's financing needs for 2026–2027 in light of Russia's ongoing war of aggression. The initiative outlines two possible solutions: (1) EU borrowing, backed by the EU budget, and (2) a Reparations Loan, based on the cash balances generated from immobilised Russian central bank assets held in the EU. Both proposals aim to ensure continued financial support for Ukraine's state budget, defence capabilities, and economic resilience. They also include safeguards designed to protect Member States and financial institutions from potential retaliatory measures linked to the use of Russian assets. The package consists of five legislative proposals, including a regulation establishing the Reparations Loan, measures preventing the return of immobilised Russian central bank assets to Russia, amendments to the EU sanctions framework, and changes to the EU's multiannual financial framework to allow the EU budget to underpin a loan to Ukraine.

■ **8 December 2025:** The Committee of Ministers of the Council of Europe examines, for the first time, the implementation of the ECtHR's judgment in the inter-state case *Ukraine and the Netherlands v. Russia*, concerning Russia's actions in eastern Ukraine since 2014 and the full-scale invasion beginning in 2022, including the downing of flight MH17. The Committee stresses that Russia remains bound by its obligations under the European Convention on Human Rights, despite no longer being a party to the Convention. It calls on CoE member states to explore all possible means to ensure the execution of the judgment and accountability for the serious violations of international law identified by the Court. The decision condemns attacks on civilians, the unlawful transfer of Ukrainian children to Russia, and the systematic use of sexual violence during the conflict. The Committee also reiterates the need for accountability for the downing of MH17 and urges Russia to acknowledge responsibility and cooperate with international efforts.

■ **15 December 2025:** The Council imposes sanctions on five individuals and four entities involved in supporting Russia's "shadow fleet" used to transport Russian oil. The targeted individuals are business figures linked to major Russian oil companies and are associated with vessels that conceal the origin of Russian crude oil while engaging in high-risk shipping practices. The sanctioned entities include shipping companies based in the United Arab Emirates, Vietnam and Russia that own or manage tankers already subject to restrictive measures for transporting Russian oil.

■ **15 December 2025:** The Council adopts sanctions against twelve individuals and two entities linked to Russia's hybrid activities, including foreign information manipulation, propaganda campaigns, and cyber-attacks targeting the EU and its partners. The measures target individuals involved in promoting pro-Kremlin narratives about Russia's invasion of Ukraine, including figures associated with institutions and networks supporting Russian state messaging.

■ **16 December 2025:** Thirty-five countries and the European Union sign a convention establishing an International Claims Commission for Ukraine. It will be established

within the framework of the Council of Europe. The new body forms part of a broader compensation mechanism addressing damage caused by Russia's war of aggression against Ukraine. It builds on the Register of Damage for Ukraine, created in 2023, which collects compensation claims submitted by individuals, organisations, and public bodies (→eucrim 1/2025, 9). The International Claims Commission will review and assess these claims and determine the amount of compensation owed in each case. The convention will enter into force once it has been ratified by at least 25 signatories and sufficient funding has been secured for its operation.

■ **18 December 2025:** The Council of the EU adopts restrictive measures against 41 additional vessels linked to Russia's so-called shadow fleet of oil tankers. The vessels become subject to a port access ban as well as a prohibition on the provision of a broad range of maritime transport services. The measure targets non-EU tankers used to circumvent the oil price cap mechanism, otherwise support Russia's energy revenues or are suspected of transporting military equipment for Russia. With the new listings, the total number of sanctioned vessels connected to Russia's shadow fleet rises to nearly 600.

■ **18/19 December 2025:** 25 Heads of State or Government adopt conclusions on Ukraine at the European Council meeting. The conclusions include, *inter alia*: Reaffirmation of the EU's continued support for Ukraine's independence, sovereignty, and territorial integrity; commitment to maintaining comprehensive political, financial, humanitarian, and military assistance; steadfast support for Ukraine's path towards EU membership; calls for a full, unconditional ceasefire by Russia; call for a continued work on a new sanctions package against Russia. EU leaders also agree to provide a €90 billion EU loan to Ukraine for 2026–2027 to support its financial and defence needs. The funding will be raised through EU borrowing on capital markets and backed by the EU budget headroom. The loan is to be implemented by enhanced cooperation as Czechia, Hungary and Slovakia declared their opt out from the financial support to Ukraine. Repayment of the loan is expected to be linked to future reparations from Russia, while Russian assets immobilised in the EU remain under consideration as a possible source for financing the support.

■ **22 December 2025:** The Council imposes restrictive measures on two members of the Russian judiciary: *Dmitry Gordeev*, a judge of the Moscow City Court, and *Lyudmila Balandina*, a state prosecutor. Both played key roles in politically motivated repressions against opposition figures, human rights defenders, and individuals critical of the Russian authorities or supportive of Ukraine.

■ **14 January 2026:** The European Commission presents a legislative package designed to secure continued EU financial support to Ukraine for the period 2026–2027 in response to Russia's ongoing war of aggression. The proposals aim to implement the European Council's political agreement of 18 December 2025 to provide €90 billion in assistance to support Ukraine's budgetary and defence needs over the next two years (see above). The package includes three main legislative proposals: (1) A new proposal establishing the €90 billion Ukraine Support Loan through enhanced cooperation, which is designed to ensure macro-financial stability in Ukraine and ease the country's external financing constraints. (2) A proposal amending the Ukraine Facility Regulation, which ensures that the funds for the Ukraine Support Loan can be channeled by the Facility. The proposal also updates the Ukraine Plan, including measures to strengthen the rule of law and the fight against corruption (conditionality mechanism). (3) Proposal amending the Regulation for the Multiannual Financial Framework 2021–2027, which will allow the coverage of the loan to Ukraine from the EU budget "headroom". The Commission also indicates that immobilised Russian assets held in the EU may be used in the future to repay the loan, while a separate proposal for a reparations loan based on these assets remains under consideration.

■ **23 January 2026:** The European Union and the Council of Europe sign an agreement to finance an advance team tasked with preparing the establishment of a Special Tribunal for the Crime of Aggression against Ukraine (→eucrim 1/2025, 9). The preparatory team will develop the institutional, logistical, and organisational foundations of the tribunal, which is intended to prosecute senior political and military leaders for the crime of aggression. The work will include preparing the election of judges and a prosecutor, drafting rules of procedure and evidence, and developing the tribunal's court management system. The project will be managed by the Council of Europe and supported with €10 million from the EU through the European Commission's Service for Foreign Policy Instruments. The preparatory phase is expected to last up to 24 months.

■ **29 January 2026:** The Council imposes sanctions on six individuals linked to Russia's hybrid activities, in particular foreign information manipulation and interference (FIMI) targeting the EU and its partners. The listings include television presenters and media figures associated with Russian state propaganda, as well as cultural personalities accused of promoting pro-Kremlin narratives about the war in Ukraine and spreading anti-Ukraine and anti-Western disinformation.

■ **29 January 2026:** The European Commission announces €153 million in humanitarian assistance to support people affected by Russia's war against Ukraine. Of this amount, €145 million is allocated to Ukraine to fund protection assistance, shelter, food, cash support, psychosocial services, and access to water and healthcare. An additional €8 million is directed to Moldova to support Ukrainian refugees hosted in the country.

■ **11 February 2026:** The European Parliament approves the legislative package enabling the €90 billion EU loan to support Ukraine for 2026–2027. The Commission tabled the package on 14 January 2026 (see above). MEPs stress that Ukraine must commit to continue democratic reforms and fight corruption as the funding is subject to strict conditions.

■ **23 February 2026:** The Council imposes restrictive measures on additional eight individuals responsible for serious human rights violations and for the repression of civil society and democratic opposition in Russia. The sanctions target members of the Russian judiciary involved in politically motivated trials against activists, as well as officials responsible for detention facilities where political prisoners were reportedly held in solitary confinement and subjected to inhuman or degrading conditions.

■ **24 February 2026:** Marking the fourth anniversary of Russia's full-scale invasion of Ukraine, European institutions condemn Russia's illegal and unjustified war of aggression against Ukraine, and reaffirm Ukraine's future in the EU. In a joint statement, the Presidents of the European Commission, the European Council, and the European Parliament highlight, inter alia, the EU's financial support to Ukraine, which has become close to €200 million since 2022. The statement also highlights ongoing efforts to ensure accountability for Russia's actions, including plans to establish the Special Tribunal for the Crime of Aggression against Ukraine and the International Claims Commission (see above). In a resolution, the European Parliament stresses that Russia and its allies are entirely responsible for the war and the ensuing crimes. MEPs call for more EU sanctions against Russia, further energy decoupling from Russian resources, and continued military, financial, and political support for Ukraine. They also recommend accelerating Ukraine's integration into the single market and accelerating EU preparations for future enlargement through internal institutional reforms.

■ **25 February 2026:** The European Commission proposes that the European Union become a founding member of the International Claims Commission for Ukraine, initiated under the umbrella of the Council of Europe on 16 December 2025 (see above).

■ **26 February 2026:** The European Commission launches the EastInvest Facility, a new financing platform aimed at supporting EU regions bordering Russia, Belarus, and Ukraine that are particularly affected by Russia's war against Ukraine. The participating financial institutions estimate that the facility could mobilise at least €28 billion in public and private investments to strengthen economic development, trade, and security in the EU's eastern border regions. (AP/TW)

Artificial Intelligence (AI)

Assessing Fundamental Rights Risks in High-Risk AI Systems

At the beginning of January 2026, the European Union Agency for Fundamental Rights (FRA) published a report focusing on the key provisions of the AI Act (→eucrim 2/2024, 92–93) and how it can be used to ensure effective protection of fundamental rights. Based on interviews with AI developers, vendors, and users, the FRA examined the challenges associated with the use of AI in critical domains, including education, employment, migration, law enforcement, and public (social) benefits.

The report covers the following aspects:

■ Defining AI;
■ Explaining what constitutes high-risk AI systems under the AI Act;
■ Outlining how to classify such systems in practice;
■ Describing how to assess high-risk AI systems with regard to fundamental rights;
■ Setting out mitigation measures;
■ Explaining how to evaluate the fundamental rights risks posed by high-risk AI systems.

Law enforcement is also a focus of the report, in particular:

■ Identifying several issues of relevance to law enforcement authorities regarding the deployment of high-risk AI systems under the EU AI Act;
■ Highlighting that AI systems used in law enforcement – such as those for risk assessment, profiling, crime analytics, or evidence evaluation – can significantly affect fundamental rights due to the power imbalance between authorities and individuals and the potential consequences for liberty, due process, and privacy.

FRA's key observations include the following:

■ Many organisations lack structured methods to assess fundamental-rights risks beyond data protection and non-discrimination;
■ There is limited consideration of rights such as the presumption of innocence, access to remedies, and fair trial guarantees;
■ Mitigation practices are fragmented and often rely heavily on human oversight, which may be ineffective if operators over-rely on AI outputs or fail to detect errors;
■ Broad interpretations of exemptions or "filters" for high-risk classification could allow law-enforcement-relat-

ed AI systems with substantial rights impacts to circumvent stricter safeguards, creating potential loopholes in protection.

Overall, the report concludes that addressing fundamental rights risks in AI requires practical guidance, effective oversight, and collaboration among all relevant stakeholders. It notes that self-assessments by AI providers and deployers are often insufficient, due to knowledge gaps and the potential for minimal compliance. There exists a need for enhanced support, research, and resources to identify, evaluate, and mitigate risks. The report emphasises that the proper implementation of the AI Act, supported by guidance, stakeholder cooperation, and empowered oversight, is essential to safeguarding fundamental rights while promoting responsible innovation and public trust. (CR)

Commission Launches AI Act Whistleblower Tool

At the end of November 2025, the European Commission launched a dedicated whistleblower tool to support the enforcement of the EU Artificial Intelligence Act. The secure reporting channel was set up within the European AI Office, the Commission's centre of expertise for AI governance, and allows individuals to report suspected breaches of the AI Act confidentially and, if desired, anonymously.

The tool was designed for individuals professionally connected to providers of general-purpose AI models or certain AI systems, including employees, contractors, shareholders, and members of management bodies. Reports can be submitted in any official EU language and supported by relevant documentation. A secure inbox system enables two-way communication with the AI Office while preserving anonymity.

According to the Commission, the tool aims to facilitate the early detection of potential violations that could endanger fundamental rights, health, safety, or public trust. The AI Office has committed to strict confidentiality standards, including certified encryption mechanisms and restricted internal access to reports. Whistleblowers receive confirmation of receipt within seven working days and are to be informed within fourteen working days whether the AI Office is competent to handle the case. Feedback on follow-up measures is to be provided within three months or, in exceptional circumstances, six months.

The Commission clarified that, until 2 August 2026, legal protection against retaliation under the EU Whistleblower Directive will not automatically apply to reports concerning infringements of the AI Act. During this interim period, confidentiality serves as the primary safeguard. From the above-mentioned date onwards, reports relating to AI Act breaches will fall within the Directive's scope. In certain cases involving product safety, consumer protection, privacy, or information security, whistleblowers can already benefit from existing protection under EU law.

The launch of the tool was presented as part of the broader implementation of the AI Act, which seeks to promote trustworthy AI while addressing systemic risks associated with high-risk and general-purpose AI models. The measure strengthens the enforcement architecture by providing an additional channel for detecting non-compliance within the emerging EU AI governance framework. (AP)

Legislation

Commission Proposes Reform of the Cybersecurity Act

On 20 January 2026, the European Commission presented a new cybersecurity package aimed at strengthening the European Union's resilience against cyber threats. The initiative included a proposal for a revised Cybersecurity Act that would repeal and replace Regulation (EU) 2019/881 and significantly expand the EU's cybersecurity governance framework.

According to the Commission, the reform responds to the rapidly evolving cyber threat landscape, marked by increasingly sophisticated attacks on critical infrastructure, businesses, and public institutions. The proposal seeks to strengthen the EU's capacity to prevent, detect, and respond to cybersecurity incidents while reducing fragmentation across the digital single market.

➤ *Reform of the Cybersecurity Act*

The proposed regulation – referred to as the "Cybersecurity Act 2" – would substantially revise the mandate of the EU Agency for Cybersecurity (ENISA). ENISA would take on expanded operational and coordination tasks, including the issuance of early alerts on cyber threats, support for responses to ransomware attacks (together with Europol and the EU CSIRTs network), and the development of vulnerability management services across the EU.

The agency would also be tasked with strengthening operational cooperation between Member States and supporting the implementation of EU cybersecurity legislation, such as the NIS2 Directive and the Cyber Resilience Act. In addition, ENISA would play a larger role in cybersecurity exercises, incident response coordination, and capacity-building initiatives aimed at strengthening the cybersecurity workforce in the EU.

➤ *Reform of the European cybersecurity certification framework*

Another central element of the reform concerned the European Cybersecurity Certification Framework (ECCF), originally introduced in 2019 but criticised for slow implementation. The proposal aimed to simplify and accelerate the adoption of certification

schemes by introducing clearer procedures and a maintenance mechanism for existing schemes.

Under the revised framework, ENISA would prepare certification schemes, which the Commission could adopt following consultation with Member States and stakeholders. Certification would remain voluntary but could serve as proof of compliance with various EU cybersecurity obligations. The framework would also expand its scope to include not only ICT products and services but also the cybersecurity posture of organisations.

The Commission argued that the updated framework would make certification a practical compliance tool for companies operating under multiple EU cybersecurity regimes while reducing regulatory fragmentation.

➤ *New EU framework for ICT supply chain security*

The reform package also introduces a new trusted ICT supply chain security framework aimed at addressing non-technical cybersecurity risks linked to suppliers. The Commission proposed a harmonised EU mechanism for identifying critical ICT assets and assessing supply chain risks, particularly where suppliers are linked to third countries posing cybersecurity concerns.

The framework would allow the Commission, following coordinated risk assessments, to designate high-risk suppliers and impose mitigation measures or restrictions on their involvement in critical ICT infrastructure. These measures could include limitations on the use of certain equipment in essential sectors or requirements to phase out high-risk components within defined transition periods.

The proposal builds on earlier initiatives such as the 5G security toolbox, extending risk-management approaches to ICT supply chains more broadly.

➤ *Simplifying compliance with EU cybersecurity rules*

In parallel with the revised regulation, the Commission also proposed targeted amendments to the NIS2 Directive to simplify compliance obligations. The changes are intended to clarify jurisdictional rules, streamline ransomware reporting, and reduce regulatory burdens for companies operating across multiple Member States.

According to the Commission, the simplification measures could reduce compliance costs for thousands of companies while improving coordination between national authorities and EU institutions.

➤ *Next steps*

The legislative package will now be negotiated between the European Parliament and the Council. (AP)

CSAM Regulation: Council Position Reached

On 26 November 2025, the Council arrived at a long-delayed position on the draft regulation to prevent and combat online child sexual abuse (CSA), signalling renewed momentum in a legislative process that had been stalled for years over privacy, encryption, and surveillance concerns.

➤ *Core elements of the Council's position*

The agreement sets out binding obligations for online platforms to assess the risk that their services could be misused for the dissemination of child sexual abuse material (CSAM) or for grooming, and it empowers national authorities to order the removal or blocking of illegal content. It also confirms the creation of a new EU agency (the EU Centre on Child Sexual Abuse) to support implementation, maintain a central database of verified CSAM indicators, and channel reports to Europol and national law enforcement.

The Council text introduces three risk categories for online services, allowing proportional obligations – particularly for high-risk platforms, which may be required to contribute to the development of mitigation technologies. Victims would be able to request the removal or disabling of content depicting them, with the EU Centre checking whether providers comply. The Council also decided to make permanent the existing temporary regime that allows providers to voluntarily scan for CSAM.

➤ *From mandatory detection orders to a softer approach*

This shift was closely linked to political developments in the Danish Council Presidency. Earlier in the year, Denmark had attempted to revive mandatory detection orders, even for end-to-end encrypted services, as foreseen in the Commission's 2022 proposal. Strong opposition from several Member States, coupled with concerns about compatibility with EU data-protection rules and the risk of mass surveillance, made an agreement in the Council impossible. In particular, the German government and the German Bar Association expressed concerns regarding the introduction of mandatory CSAM detection orders for online platforms, including services protected by end-to-end encryption. In autumn 2025, Denmark formally abandoned the push for mandatory scanning and steered the Council toward a compromise centred on voluntary detection and risk-mitigation obligations.

The Council's position also brought the file back full circle to the Commission's original proposal of May 2022, which had been framed as a response to the rapid growth of online CSAM and the inadequacy of the voluntary-only system in place at the time. As reported by eucrim (→ eucrim 2/2022, 91–92), the 2022 draft regulation was conceived as a comprehensive framework combining two elements:

- Obligations for providers to detect, report, remove, and block CSAM;
- The establishment of the EU Centre

as a decentralised agency providing verified indicators, technological support, and operational coordination.

However, the detection-order mechanism at the heart of the original proposal quickly became the focal point of intense criticism, with NGOs, academics, privacy advocates, and several Member States warning that it risked creating a de facto system of blanket communications surveillance, including within encrypted channels (→eucrim 1/2023, 13–14).

➤ *Next steps*

The Council's 2025 position reflects this debate. It preserves the structural elements of the 2022 proposal – risk assessment, risk mitigation, removal orders, oversight mechanisms, and the EU Centre – while deliberately excluding mandatory detection orders. The latter is in conflict with the Commission's and European Parliament's position (the EP had already adopted its position in 2023 (→eucrim 3/2023, 246)). Trilogue negotiations started on 9 December 2025.

In parallel, on 19 December 2025, the Commission tabled a proposal to extend the interim regulation governing the voluntary control of child abuse content (which expired on 3 April 2026) until 3 April 2028. Update: On 26 March 2026, the EP rejected the proposal by 228 to 311 votes. This means that the temporary regulation expired after 3 April 2026. As a result, online platforms are now exempt from the requirement to voluntarily and proactively monitor chats; there is no longer an exception to the e-Privacy Directive.

The Commission proposal for long-term rules to prevent and combat child abuse is currently one of the most controversial legislative dossiers in Brussels in the area of justice and home affairs. The European Parliamentary Research Service (EPRS) is monitoring the debate and provides regular updates on the different positions. (AP)

Digital Space Regulation

EU Fines X €120 Million in First DSA Non-Compliance Decision

On 5 December 2025, the European Commission imposed a €120 million fine on X after concluding that the platform had breached several transparency duties under the Digital Services Act (DSA). This is the first non-compliance decision adopted since the DSA entered into force.

➤ *The Commission's conclusion*

The Commission determined that X had violated three core obligations:

- X's paid "blue checkmark" feature deceives users increasing their exposure to scams, including impersonation fraud;
- X's advertising repository is insufficiently transparent and unreliably accessible preventing researchers and civil-society organisations from effectively examining potential threats;
- X's terms of service bar independent collection of public information, such as scraping, and its formal access procedures create additional hurdles undermining research into systemic risks in the EU that the DSA aims to address.

The €120 million fine reflects the seriousness and duration of the violations, as well as the number of EU users affected.

The Commission concluded that each of the practices at issue directly conflict with the transparency and accountability standards that very large online platforms (VLOPs) must meet under the DSA. In particular, the deceptive presentation of the checkmark constituted an unlawful design practice; the deficiencies in the ad repository fell short of the strict disclosure rules in Art. 39; and X's obstacles to data access violated Art. 40(12), which guarantees researchers the ability to study risks that may affect EU society.

➤ *Next steps and implications*

X was given 60 working days to explain how it would put an end to the deceptive use of blue checkmarks and 90 working days to submit a full action plan addressing the shortcomings in its ad repository and researcher access systems. The Digital Services Board will provide an opinion once the plan has been submitted, after which the Commission will set a compliance deadline. Continued violations may trigger additional periodic penalties.

The Commission also signalled that this case forms only part of a wider investigation into X's handling of illegal content and information manipulation, launched in December 2023 and which is still ongoing.

In a statement, Executive Vice-President *Henna Virkkunen* stressed that the decision demonstrates the EU's resolve to hold major platforms accountable: the DSA, she said, is intended to protect users, support independent research, and restore trust in online environments. (AP)

Overview of the Latest Developments under the Digital Services Act: November 2025 – February 2026

Eucrim regularly reports on the EU's new major legislation regulating the digital space, i.e., the Digital Services Act and the Digital Markets Act (→eucrim 1/2024, 12–13 with further references). The Digital Services Act (DSA) is designed to foster a safer, fairer, and more transparent online environment (→eucrim 4/2022, 228–230). It establishes new obligations for online platforms, thereby ensuring that EU users are safeguarded against the dissemination of illicit goods and content and that their rights are respected when they engage in interactions, share information, or make purchases online. The DSA is also highly relevant for law enforcement purposes (→eucrim 1/2024, 13).

This news item continues the reporting on the latest DSA developments by giving a chronological overview. It covers the period from November 2025 to February 2026. For overviews of previous developments,

see: November 2024 – January 2025 →eucrim 4/2024, 272–273; February–April 2025 →eucrim 1/2025, 12–13; and May to Mid-October 2025 →eucrim 2/2025, 120–122 – each with further references.

■ **12 November 2025:** The European Commission presents the European Democracy Shield, which includes several measures directly relevant to the DSA. To safeguard the integrity of the information space, the Commission prepares a DSA incidents and crisis protocol to facilitate coordination among competent authorities in cases of large-scale or cross-border information manipulation. It also works with signatories of the Code of Conduct on Disinformation within the DSA framework. The initiatives reinforce the DSA's role as a key instrument for addressing systemic risks, including disinformation and foreign information manipulation, while enhancing cooperation between EU institutions, Member States, and relevant stakeholders.

■ **18 November 2025:** The European Board for Digital Services, in cooperation with the Commission, publishes its first annual report under Art. 35(2) of the DSA, identifying the most prominent and recurrent systemic risks linked to Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). The report highlights recurring systemic risks in four main areas: (1) the dissemination of illegal content (including illegal products, terrorist content, CSAM, and hate speech); (2) impacts on fundamental rights (notably freedom of expression, non-discrimination, privacy, and consumer protection); (3) risks to civic discourse, elections, and public security (including disinformation, foreign information manipulation, and algorithmic amplification); and (4) risks related to gender-based violence, public health, the protection of minors, and mental well-being. The Board underlines that systemic risks concern platform design, functioning, and large-scale effects rather than individual pieces of content. It emphasises the central role of Arts. 34 and 35 DSA, requiring VLOPs and VLOSEs to assess and mitigate systemic risks in a proportionate manner, with particular regard to fundamental rights. The report also outlines mitigation practices currently in use or proposed, including adjustments to content moderation systems, recommender systems and advertising systems, as well as the use of trusted flaggers, transparency tools, and codes of conduct.

■ **26 November 2025:** The Commission sends a request for information (RFI) to Chinese multinational online clothing retailer *Shein* under the DSA, following indications that illegal products – including child-like sex dolls and weapons – are being offered on the platform. The Commission asks Shein, designated as a VLOP, to provide detailed information and internal documents on how it prevents the sale of illegal goods and how it protects minors from exposure to age-inappropriate content, including through age assurance measures. It also seeks clarification on the effectiveness of Shein's risk mitigation systems. This is the third RFI that the Commission sent to Shein.

■ **27 November 2025:** In his speech *"Trusted Sources of Information in a Democratic Society"* delivered on 27 November 2025 in Brussels to the Citizens Information Board, Commissioner *Michael McGrath* underlines the central role of the DSA in safeguarding the integrity of the information space. He stresses that the DSA requires VLOPs to assess and mitigate systemic risks, including coordinated inauthentic behaviour and disinformation risks linked to recommender systems. The Commission has issued DSA guidelines to mitigate risks to electoral processes, and several DSA investigations remain ongoing. Looking ahead, the Commission is preparing a DSA incidents and crisis protocol, together with the European Board for Digital Services, to strengthen coordination in response to major information manipulation incidents.

■ **5 December 2025:** The European Commission fines X 120 million Euro for breaching its obligations under the DSA. This marks the first non-compliance decision adopted under the DSA. The Commission finds that X violates Art. 25(1) DSA by using a misleading "blue checkmark" design. Because users can obtain verified status through payment without meaningful identity verification, the platform creates a deceptive impression of authenticity, contrary to the DSA's prohibition of deceptive design practices. The Commission also finds infringements of Art. 39 DSA due to deficiencies in X's advertising repository. The repository lacks key transparency elements, including clear information on ad content and the paying entity, and contains access barriers that undermine scrutiny by researchers and civil society. In addition, X breaches Art. 40(12) DSA by failing to provide researchers with effective access to public data. X must now submit corrective measures within set deadlines. Failure to comply may result in periodic penalty payments. The Commission states that investigations concerning other potential DSA breaches by X remain ongoing.

■ **5 December 2025:** The Commission accepts binding commitments from TikTok to address concerns regarding advertising transparency under the DSA. Following preliminary findings in May 2025 (see →eucrim 2/2025, 120–122), TikTok commits to ensure that its advertising repository fully complies with DSA requirements. The platform will provide, *inter alia*, the complete content of advertisements as shown to users, including embedded URLs, and will update

its repository within 24 hours. TikTok must implement the commitments within agreed deadlines of up to 12 months. The Commission will monitor compliance under Art. 71 DSA. Other DSA investigations concerning TikTok – including recommender systems, age assurance, data access for researchers, protection of minors, and election-related risks – remain ongoing.

■ **26 January 2026:** The Commission launches a new formal investigation against X under the DSA (Arts. 34, 35, and 42 relating to risk assessment, mitigation, and independent auditing obligations). The investigation focuses on risks linked to the deployment of the AI tool Grok within the platform. In parallel, it extends its ongoing proceedings from December 2023 concerning X's recommender systems. The Commission assesses whether X has properly identified and mitigated systemic risks arising from Grok's integration, including the dissemination of illegal content such as manipulated sexually explicit images and potential child sexual abuse material. It also examines whether X conducted and submitted an ad hoc risk assessment prior to deploying Grok functionalities that significantly affect its risk profile.

■ **10 February 2026:** Under the Action Plan Against Cyberbullying, the Commission announces several measures directly linked to the DSA. The Commission will review the DSA guidelines on the protection of minors to strengthen the obligations of online platforms to prevent minors from being exposed to harmful content and to ensure that reporting mechanisms are easily accessible. It will also adopt DSA guidelines on trusted flaggers to clarify their role in addressing illegal content, including illegal cyberbullying content. According to the Action Plan, the DSA requires online platforms to ensure a high level of privacy, safety, and security for minors and to mitigate systemic risks related to harmful content.

■ **17 February 2026:** The Commission opens formal proceedings against Shein under the DSA. The investigation concerns whether the platform has adequate systems to prevent the sale of illegal products in the EU, including content that may constitute child sexual abuse material. The Commission also examines whether Shein's design features, such as reward-based engagement mechanisms, create addictive effects and whether the company properly assesses and mitigates related systemic risks. In addition, it reviews compliance with DSA transparency obligations for recommender systems, including disclosure of main ranking parameters and the requirement to offer users at least one option not based on profiling. (AP)

Overview of the Latest DMA Developments: November 2025 – February 2026

Eucrim regularly reports on the EU›s major new legislation regulating the digital space, i.e., the Digital Services Act and the Digital Markets Act (→eucrim 1/2024, 12–13 with further references). The Digital Markets Act (DMA) aims to ensure contestable and fair markets in the digital sector (→eucrim 4/2022, 228–230). It regulates gatekeepers: large digital platforms that provide an important gateway between business users and consumers. Their position can grant them the power to act as bottlenecks in the digital economy.

The following is an overview of the latest developments since the news on the DMA in →eucrim 2/2025, 122 (covering the period May – October 2025). For other overviews, →eucrim 1/2025, 13–14 (covering the period January – April 2025) and →eucrim 4/2024, 178–179 (covering the period October–December 2024).

■ **13 November 2025:** The European Commission opens formal proceedings to assess whether Alphabet Inc. complies with its obligations under the DMA in relation to the treatment of media publishers in Google Search. The investigation focuses on Google's "site reputation abuse policy", which may demote publishers' websites in search results when they host content from commercial partners. The Commission is examining whether this practice could undermine fair, reasonable, and non-discriminatory access to Google Search, potentially affecting publishers' ability to monetise their content and cooperate with third-party providers. The opening of proceedings does not prejudge the outcome of the case. If the Commission ultimately finds an infringement of the DMA, it may impose fines of up to 10% of the company's global turnover, or up to 20% in the event of repeated violations, alongside additional remedies.

■ **18 November 2025:** The Commission opens three market investigations under the DMA concerning the cloud computing sector. Two investigations will assess whether Amazon and Microsoft should be designated as gatekeepers for their cloud services Amazon Web Services and Microsoft Azure, despite these services not meeting the quantitative DMA thresholds. The Commission will examine whether the two platforms function as key gateways between businesses and users and whether structural features of the cloud market reinforce their strong market positions. If designated as gatekeepers, the services would be added to the list of core platform services already covered by the DMA. A third investigation will examine whether the DMA effectively is addressing potentially unfair or anti-competitive practices in the cloud sector, including interoperability barriers, restricted access to data, bundling of services, and imbalanced

contractual terms. The Commission aims to conclude the gatekeeper investigations within twelve months.

■ **8 December 2025:** Meta Platforms commits to offering EU users a choice between different advertising models on Facebook and Instagram to comply with the DMA. Under the new approach, users can either consent to the use of their data for fully personalised advertising or opt for a version of the services based on more limited data sharing and reduced personalisation.

■ **12 December 2025:** The High-Level Group on the Digital Markets Act holds its fifth meeting to discuss cooperation between authorities responsible for enforcing the EU's digital regulatory framework. The discussion focuses on how different legal instruments of the EU *digital acquis* can be applied in a coordinated way in digital markets. The group also endorses a joint paper on artificial intelligence that maps regulatory interactions affecting AI across the EU framework, including competition, data protection, consumer protection, and platform regulation. The paper highlights concerns about contestability and fairness in the AI value chain, noting that major digital gatekeepers increasingly integrate AI systems into their ecosystems and control key infrastructure such as cloud services and access to data. To address these challenges, the High-Level Group calls for stronger cooperation between regulators and mandates its AI sub-group to continue work on cross-regulatory coordination in the development and deployment of AI systems by gatekeepers.

■ **8 January 2026:** The Commission publishes a summary and individual contributions submitted in the consultation for the first review of the Digital Markets Act. More than 450 submissions were received from a broad range of stakeholders, including SMEs, digital platforms, civil society organisations, academics, and individual citizens. Most respondents support the DMA's objective of ensuring fair and contestable digital markets, while also highlighting implementation challenges. Many contributions call for stronger interoperability, improved data access and portability, and greater support for SMEs. Several respondents also suggest expanding the regulation's scope, particularly with regard to artificial intelligence and cloud services. By contrast, gatekeepers raise concerns about proportionality, compliance costs, and potential impacts on user experience. The consultation results will inform the Commission's review report on the DMA, which must be presented to the European Parliament, the Council, and the European Economic and Social Committee by May 2026.

■ **27 January 2026:** The Commission opens two specification proceedings under the DMA to clarify how Google must comply with certain interoperability and data-sharing obligations. The first proceeding concerns interoperability obligations related to the Android operating system. The Commission will specify how Google should ensure that third-party developers, including providers of AI services such as those competing with Gemini, can access hardware and software features on equal terms with Google's own services. The second proceeding concerns Google's obligation to provide third-party search engines with access to anonymised ranking, query, click and view data from Google Search on fair, reasonable, and non-discriminatory terms. The Commission will examine issues such as the scope of data sharing, anonymisation methods, and whether AI chatbot providers should be eligible to access the data. The proceedings formalise the Commission's regulatory dialogue with Google and aim to clarify compliance requirements within six months. They do not prejudge whether Google is in breach of the DMA.

■ **5 February 2026:** The Commission concludes that Apple Ads and Apple Maps should not be designated as core platform services under the DMA. The decision follows a notification submitted by Apple in November 2025. After reviewing the company's arguments, the Commission determined that neither service qualifies as an important gateway between business users and end users. The assessment notes, in particular, the relatively low usage of Apple Maps in the EU and the limited scale of Apple Ads in the online advertising market. The decision does not affect Apple's existing designation as a gatekeeper for other core platform services under the DMA. (AP)

Institutions

Council

"Autonomous and Open": Cyprus' Vision for EU Council Presidency

As the third Member State in the current Trio Presidency after Poland and Denmark, Cyprus assumed the Presidency of the Council of the EU from 1 January 2026.

Under the motto "An Autonomous Union. Open to the World", the Cypriot Presidency is striving to promote a more autonomous Europe through enhanced security, defence readiness, and preparedness. In this spirit, it is supporting key defence initiatives such as the implementation of the White Paper on the Future of European Defence and the accompanying Readiness Roadmap 2030, as well as the EU Maritime Security Strategy.

Critical dimensions of security form an integral part of the Presidency's agenda:

■ Economic security as a core pillar of the programme, with the Presidency steering the implementation of the 2023 Economic Security Strategy;

- Water resilience, migration management, protection against attacks on democracy, and the fight against discrimination;
- Strengthening strategic autonomy through competitiveness, which includes completing the Single Market, boosting Europe's financial economy, strengthening energy security, and enhancing Europe's digital sovereignty;
- Continuing efforts to establish the Multiannual Financial Framework for 2028–2034 (MFF).

The Presidency also aims to reinforce the EU's role as a strategic global actor by advancing the enlargement agenda. In the area of Justice and Home Affairs, the Cypriot Presidency has the following aims:

- To enable the EU to effectively manage its external borders, protect its citizens from internal and external threats, and uphold fundamental rights;
- To continue to advance the JHA agenda for effective migration management, with a strong focus on the implementation of the Pact on Migration and Asylum and the development of comprehensive partnerships with third countries;
- To consolidate a well-functioning Schengen area by closely monitoring the operation of the European Entry/Exit System (EES), supporting progress towards the launch of the European Travel Information and Authorisation System (ETIAS), and continuing trilogue negotiations on the Regulation establishing the Digital Travel Credentials Application;
- To further pursue cooperation with the United States, the Western Balkans, and Latin America.

The internal security of the Union will also be further strengthened as follows:

- Enhancing law-enforcement capabilities and deepening cooperation among Member States and EU agencies;
- Leading discussions on the forthcoming proposal to transform Europol into a more operational law enforcement agency and by launching negotiations on the reform of Eurojust;
- Addressing transnational and organised crime, including through efforts to deprive criminal networks of their illicit proceeds, while tackling emerging threats stemming from technological developments;
- Placing particular emphasis on better protecting minors from both online and offline threats;
- Giving priority to negotiations on the Directive to combat child sexual abuse, the Regulation preventing and combating child sexual abuse, and the reform of the European Investigation Order (EIO);
- Combating organised crime, migrant smuggling, drug trafficking, terrorism, violent extremism, and trafficking in cultural property;
- Addressing drug trafficking within the framework of the new EU Drugs Strategy and the EU Action Plan against Drug Trafficking, with equal emphasis on demand and supply reduction;
- Exploring alternative approaches for young people in conflict with the law.

The Cypriot Presidency will end on 30 June 2026 and will be followed by a new Trio Presidency, beginning with Ireland, followed by Lithuania and Greece. (CR)

Court of Justice of the European Union (CJEU)

CJEU: New Website, Search Engine, and Web TV

At the beginning of 2026, the Court of Justice of the European Union modernised its digital communication to enhance openness, transparency, and accessibility for both the general public and legal professionals. This initiative includes:

- The launch of a fully redesigned website;
- An upgraded and more powerful search engine (InfoCuria);
- A new audiovisual platform (CVRIA Web TV).

For the new website, particular emphasis was placed on a user-friendly information structure, an intuitive web design that facilitates navigation and meets high accessibility standards, and clear language that is easily understood by both professionals and the general public.

The updated search engine, InfoCuria, is being introduced in two phases. The first phase, designed specifically for non-experts, offers a user-friendly and accessible interface, enabling faster and easier access to information with new features: fuzzy search, Boolean operators, auto-completion, faceted search, relevance-based sorting, and keyword highlighting. The second phase, currently under development, is intended for experts and will allow more targeted searches based on a wide range of criteria: the referring court, type and outcome of proceedings, composition of the panel, Advocate General, and Judge-rapporteur.

The CVRIA Web TV programme is aligned with the Court's calendar and includes live broadcasts when judgments are delivered. It also features the reading of opinions, reports on oral hearings, delayed broadcasts of hearings, and explanatory contributions by members of the Court. In addition, three new programmes have been produced, which will be broadcasted regularly on the platform:

- *La Cour des citoyens*, an educational programme, which explains the role and responsibilities of the Court and illustrates the real-life impact of its decisions;
- *Open Court,* an interview programme, in which members of the Court inform about its working methods and other key issues;
- *Bright,* an entertaining short-form programme, which focuses on specific

areas of everyday life and explains in a clear and accessible manner how they are shaped by the Court's case law.

Together, these innovations will strengthen the Court's role as a transparent judicial authority of the European Union and make its activities and decisions more readily available and easier to understand for Union citizens. (CR)

OLAF

OLAF Operational Work: September–December 2025

This news item highlights key cases that demonstrate OLAF's operational work between 1 September 2025 and 15 January 2026. It follows reports on operations supported by OLAF in the first seven months of 2025 (→eucrim 2/2025, 125–126), including the Office's cooperation with the EPPO. The following overview is in reverse chronological order.

■ **8 January 2026:** OLAF reports that it finalised an investigation that revealed systemic weaknesses in the management of EU funds in Hungary. The investigation concerned the funding of projects for tourism and sustainability under the European Agricultural Fund for Rural Development (EAFRD). It was opened in March 2023 and closed in December 2025. OLAF detected a series of manipulated public procurement procedures and inflated prices for supplies. Administrative recommendations were issued; national criminal proceedings relating to the projects are ongoing. Approximately €500,000 was prevented from being unduly spent thanks to OLAF.

■ **18 December 2025:** A joint operation between OLAF and the French Customs results in the seizure of more than 10.7 million counterfeit toys sold online. After the French Customs reported initial discoveries, OLAF launched a coordinated investigation at European level. It brought together the Member States concerned to harmonise the investigation strategy, then supervised several months of online investigations, conducted jointly with French and Czech customs. It also closely collaborated with online platforms on which the illicit toys were sold by third parties. Further joint operations to combat counterfeit and dangerous products sold online will follow.

■ **30 October 2025:** OLAF informs the public of the results of Operation NOXIA II. This operation targets deep-sea containers in EU and Asian ports in a bid to prevent the smuggling of illicit cigarettes and dangerous substances. The first edition was conducted in 2023 (→eucrim 4/2023, 318). Operation NOXIA II resulted in the coordinated seizure of 149.5 million cigarettes, over 3,000 tonnes of illicit waste, 66.5 kg of pseudoephedrine, 52 tonnes of solid pesticides, and 21,000 litres of liquid pesticides. Under the lead of OLAF, this joint customs operation involved 40 European and Asian countries. OLAF stresses that the Operation has also fostered a network of like-minded investigators, aiming to set up a regular information exchange between the EU and Asia through the Asia-Europe Meeting (ASEM).

■ **24 October 2025:** A customs operation monitored by OLAF leads to the seizure of 12 tonnes of illegal F-gases in south-east Spain. Acting on intelligence provided by OLAF, the Spanish authorities confiscated a truck carrying cylinders, worth around 413,000 euros. OLAF also identified the smugglers' international routes, as F-gases are typically imported to the EU from non-EU countries. F-gases are strictly regulated in the EU due to their impact on global warming, yet the black market continues to expand. Combatting the smuggling of illicit F-gases is one of OLAF's key priorities.

■ **24 September 2025:** OLAF reports that one of its first complementary investigations for the EPPO resulted in convictions of main perpetrators in Croatia. The investigation involved procurement fraud in relation to the purchase of an information system by the Croatian Ministry for Regional Development and EU Funds (MRRFEU). The purchase was co-financed by the European Regional Development Fund. The former minister of the MRRFEU was sentenced to two years of imprisonment in June 2025. In September 2025, one of two business owners involved in the case was convicted as well. The EPPO took over the case from OLAF in 2022. OLAF revealed that the public authority and the economic operator may have colluded to inflate the value of the public procurement procedure and ensure that the contract was awarded to the predetermined economic operator. OLAF also recommended the recovery of €1.4 million to the European Commission, while the EPPO indicted several high-ranking officials and businessmen in Croatia. (TW)

European Public Prosecutor's Office (EPPO)

Andrés Ritter Succeeds *Laura Kövesi* as European Chief Prosecutor

spot light

On 10 March 2026, the European Parliament approved the appointment of *Andrés Ritter* as the next European Chief Prosecutor, following the agreement of the Council of the EU. His mandate will commence on 1 November 2026. He will succeed *Laura Codruța Kövesi*, the European Public Prosecutor's Office's first Chief Prosecutor, whose non-renewable seven-year term expires on 31 October 2026.

The selection of the European Chief Prosecutor (ECP) is quite transparent, starting with the publication of an open call for applications in the Official Journal of the EU. Then, the appointment requires the agreement of both the European Parliament and

the Council. As a third step, the European Parliament conducts public hearings of candidates shortlisted by a 12-member selection panel composed of former members of supranational judicial bodies, including the Court of Justice of the EU, the Court of Auditors of the EU, and Eurojust, as well as national supreme court judges, senior prosecutors, and lawyers of recognised competence. Information on candidates, including their responses to a parliamentary questionnaire, is made publicly available. In contrast, proceedings within the Council are not public; no hearings or detailed statements are disclosed, and the Council determines its preferred candidate prior to entering into negotiations with the Parliament.

Pursuant to Art. 14(2) of the EPPO Regulation, candidates for the position of ECP must be active members of a national prosecution service or judiciary or serving European Prosecutors. They must demonstrate unquestionable independence, qualifications equivalent to those required for the highest prosecutorial or judicial offices in participating Member States, and they must have experience in financial crime and international judicial cooperation in criminal matters. In addition, candidates must possess adequate managerial experience.

In April 2025, a call for candidates for the position of European Chief Prosecutor was published in the Official Journal (→eucrim 1/2025, 20–21). Seventeen applications were received. The selection panel shortlisted four candidates: *Andrés Ritter* (Germany), *Ingrid Maschl-Clausen* (Austria), *Emilio Jesús Sánchez Ulled* (Spain), and *Stefano Castellani* (Italy).

On 3 December 2025, the four shortlisted candidates presented their candidacies in a Q&A session with MEPs. In the session, *Andreas Ritter* emphasized the importance of strengthening cooperation with national authorities as well as Europol, OLAF, Eurojust, and AMLA in order to achieve shared objectives while avoiding duplication and competition. He referred to the ongoing revision of the relevant regulations in this context. He also stressed the need to contribute to asset confiscation and highlighted new opportunities for cooperation with AMLA. Mr Ritter emphasized the importance of tackling corruption without fear or hesitation. When asked about potential new competences, he underlined that it is ultimately up to the legislator to decide whether the EPPO model should be extended to cover additional crimes. Following the hearing, MEPs voted on their preferences, with Mr *Ritter* emerging as the preferred candidate. On 23 February 2026, the EP's Committee on Civil Liberties, Justice and Home Affairs (LIBE) voted to support his appointment as head of the EPPO, with 52 votes in favour, 10 against, and 6 abstentions.

Andrés Ritter joined the prosecution service of the Federal Republic of Germany in 1995 and was appointed Deputy Prosecutor General in Mecklenburg-Western Pomerania in 2008. He subsequently led several public prosecution offices, including serving as Chief Prosecutor of the specialised Public Prosecution Office for Economic Crime and Cybercrime in Rostock, Germany, from 2013 to 2020. Prior to his appointment as Germany's first European Prosecutor, he has served for five years as one of the two Deputy European Chief Prosecutors – a role he continues to hold until 31 October 2026. (CR)

EPPO College Partial Renewal in 2026

On 11 February 2026, the Council appointed two new European Prosecutors to the EPPO: *Jennifer Vanderputten* for Belgium and *Pavel Zeman* for the Czech Republic. *Jennifer Vanderputten* has been European Delegated Prosecutor and EPPO's coordinator for the Brussels office. She is also a specialised lawyer in commercial law. *Pavel Zeman* was national member for the Czech Republic at Eurojust from 2004 to 2011 and again from 2025 to 2026. He also served as a public prosecutor at the international department of the Supreme Public Prosecutor's Office. The two new prosecutors are appointed for a non-renewable term of six years, from July 2026.

At the end of July 2026, the mandates of five other European Prosecutors (from Bulgaria, France, Malta, Slovenia, and Slovakia) will end. The nomination process is part of the rotation system of European Prosecutors at the EPPO's central office in Luxembourg: one third of European Prosecutors are renewed every three years. To ensure continuity, the mandates of seven prosecutors (from Germany, Estonia, Croatia, Latvia, Luxembourg, Romania, and Finland) were extended until 30 June 2029, following a draw in April 2024.

Regarding the partial renewal of now seven European Prosecutors, each participating Member State concerned nominates three candidates for the respective replacement of the country's European Prosecutor. A selection panel composed of 12 members, including former EU judges, auditors, senior prosecutors, and lawyers (one of whom is proposed by the European Parliament), assesses the candidates, issues reasoned opinions, and ranks those who meet the selection criteria. The Council then appoints one candidate per Member State.

European prosecutors supervise investigations and prosecutions. Together with the European Chief Prosecutor, they form the EPPO College. (CR)

EPPO and OLAF Investigate Alleged Fraud Linked to EU Diplomatic Academy

At the beginning of December 2025, the European Public Prosecutor's Office (EPPO) in Brussels conducted

searches in several buildings of the College of Europe in Bruges, at the European External Action Service in Brussels, and at the homes of three suspects in connection with alleged fraud relating to EU-funded training for junior diplomats. The investigative measures were carried out with the support of OLAF.

The investigation concerns the European Union Diplomatic Academy, a nine-month training programme for junior diplomats from the Member States. It was awarded to the College of Europe in Belgium for the period 2021–2022 by the European External Action Service (EEAS) following a tender procedure. The investigation's focus is on whether the College of Europe and/or their representatives were informed in advance about the selection criteria for the tender procedure and had sufficient reason to believe that they would be awarded the implementation of the project prior to official publication of the tender notice by the EEAS.

Before the searches took place, the EPPO requested that the immunity of several suspects be lifted, which was granted. The rector and a senior staff member of the College of Europe as well as a senior official of the European Commission were detained. The accusations concerned procurement fraud and corruption, conflict of interest, and breach of professional secrecy. (CR)

Publication on Strengthening the Future of the EPPO

Compiling contributions from academics, legal practitioners, and officials from public authorities, the collective book "Strengthening the Future of the European Public Prosecutor's Office" is available open access in the library of publisher *Nomos*. The contributions build on discussions held during workshops at the *Villa Vigoni,* Lago di Como, which is part of the German-Italian Centre for European Dialogue (see the conference report by *L. Jakobi* and *G. Theodorakakou* in eucrim 1/2025, 51–62).

The publication, edited by *Dominik Brodowski* and *Sebastian Trautmann*, provides substantive insights into the work, constraints and role of the EPPO in the EU area of freedom, security and justice within the current framework. It also offers suggestions for the institution's future positioning. They may feed into the upcoming EU-level discussion about adjusting the 2017 EPPO Regulation. (TW)

Europol

New Amending Europol Regulation in Force

On 22 December 2025, Regulation (EU) 2025/2611 amending Regulation (EU) 2016/794 as regards the strengthening of Europol's support and enhancing police cooperation, for preventing and combating migrant smuggling and trafficking in human beings, was published in the Official Journal of the EU (*OJ L, 2025/2611*).

After three years of negotiations, the legislation to strengthen Europol's mandate with regard to preventing, detecting, and investigating migrant smuggling and trafficking in human beings (THB) was finalized and entered into force on 11 January 2026. For the provisional agreement between the Council and the European Parliament, →eucrim 3/2025, 197–198. For the Commission proposal as part of the legislative package to counter migrant smuggling, →eucrim 3/2023, 257–258.

Key features of the amending Regulation are:

- Stronger obligations for the national authorities of EU Member States to share relevant information on migrant smuggling and human trafficking with Europol in a timely manner;
- EU Member States may also establish operational task forces for the duration of specific criminal intelligence activities or investigations, and Europol shall facilitate and support their implementation;
- Member States may request Europol deployment on their territories for operational support, under certain conditions and in accordance with their national laws;
- Strengthening of the European Centre Against Migrant Smuggling, which will become a permanent part of Europol's structure.

As an EU Regulation, the Regulation is binding in its entirety and directly applicable in all EU Member States. (CR)

Europol and Argentina Sign Working Arrangement

On 1 December 2025, Europol and the Republic of Argentina signed a Working Arrangement to enhance cooperation in combating cross-border crime.

The arrangement establishes a structured legal framework for collaboration and the exchange of non-personal information between Europol and Argentine law enforcement authorities. It is expected to facilitate joint efforts in areas such as organized crime, drug trafficking, human trafficking, cybercrime, and environmental crime. The arrangement also allows for the sharing of specialist knowledge, general situation reports, and strategic analysis as well as participation in training activities and the providing of support for individual criminal investigations.

Under the terms of the arrangement, Argentina will designate a national contact point to support cooperation with Europol. Provisions are included for the potential deployment of liaison officers to Europol. (CR)

Europol Report on the Impact of Robotics and Unmanned Systems on Law Enforcement

Recent conflicts, including the ongoing Russian war of aggression against Ukraine, have accelerated the develop-

ment and deployment of advanced unmanned systems. The lessons learned from the use of these systems are of particular relevance to European law enforcement agencies as they prepare for an evolving operational environment.

On 8 December 2025, Europol's Innovation Lab published a report providing an in-depth analysis of how unmanned systems may reshape society, criminal activity, and law enforcement. The report addresses, *inter alia*, the following:

- The increasing use of unmanned systems;
- Technical and regulatory challenges arising from their deployment;
- Emerging security threats;
- The need to ensure public trust through appropriate regulatory frameworks;
- The implications of operating in a three-dimensional environment encompassing air, ground, and underwater domains.

The report identifies 2022 as a turning point, marking the year in which organised crime began using unmanned systems across all domains with a new form of "crime-at-a-distance" emerging from today's "crime-as-a-service".

The report sets out the following challenges for legal regulations and practical reactions by the police:

- Unmanned systems are operating over increasingly vast distances;
- They are acting with growing autonomy and coordination;
- They are becoming progressively more capable;
- They increase rapidly in number and variety.

With regard to the current use of unmanned systems in law enforcement, the report highlights the deployment of drones, robots, and other autonomous technologies for surveillance and reconnaissance, crime scene mapping and forensic analysis, search and rescue operations, and the disposal of explosive ordnance and hazardous materials. The limitations of existing systems include their restricted level of autonomy, task-specific specialization, limited battery life, and, importantly, a lack of independence from industrial suppliers.

Concerning the threat from unmanned systems, the report notes that law enforcement's capability to counter the use of unmanned systems by criminals at scale remains limited. The disparity between the evolving threat and the capacity to mitigate and protect against it has widened into a significant gap. This gap is not only technological in nature but also extends to regulatory frameworks, training, data sharing, and infrastructure.

In its final chapter, the report outlines a series of recommendations for European law enforcement authorities. It concludes that the rapid integration of increasingly capable unmanned systems will profoundly transform society and law enforcement, expanding the scope of policing and challenging traditional practices. While these technologies present new security risks and may be exploited by criminal actors, they also offer significant operational benefits if supported by robust regulation, public trust, and strategic investment. To ensure technological autonomy and achieve desirable outcomes, European stakeholders must act proactively, strengthen research and innovation, and adapt decision-making to the pace of technological change. (CR)

Frontex

ECJ Rules on Frontex Obligations in Joint Return Operations and Pushbacks

spot light

On 18 December 2025, the ECJ issued two judgments on Frontex activities in joint return operations (Case C-679/23 P, *WS and Others v Frontex*) and pushbacks (Case C-136/24 P, *Hamoudi v Frontex*). Upon appeal, the Grand Chamber of the ECJ largely set aside the judgments of the General Court and referred the cases back to it.

➤ *Background of the cases*

Both cases were brought by Syrian nationals who, despite having expressed a desire for asylum, were relocated to Türkiye as part of a joint return operation and a pushback, both supported by Frontex, after their arrival in Greece. Taking the view that their transfer to Türkiye constituted an unlawful refoulement and that their fundamental rights were infringed during that transfer, they applied to the General Court of the EU to order Frontex to pay compensation for the material and non-material damage allegedly caused by the agency's conduct. The General Court dismissed the actions in both cases.

Regarding the joint return operation, the General Court argued that there was no causal link between the allegedly illegal conduct of Frontex and the damage suffered, without assessing the other conditions for liability. It held that, since Frontex had no competence as regards either the assessment of the merits of return decisions or the examination of applications for international protection, it could not be held liable for any damage connected with the return of those persons to Türkiye (Case T-600/21, *WS and Others v Frontex*).

Regarding the pushback by Frontex, the General Court argued that the evidence produced by the applicant did not demonstrate conclusively that he had been present at the pushback (CaseT-136/22, *Hamoudi v Frontex*).

➤ *The joint return operation case*

Looking at the appeal in the case of the joint return operation, the ECJ held that EU law imposes on Frontex a set of obligations intended to ensure respect for fundamental rights in the context of joint return operations. It reiterated that joint return operations

may concern only those persons who have been the subject of enforceable written return decisions. In detail:

- Frontex is required to verify that such decisions exist for all the persons whom a Member State intends to include in joint return operations, in order to ensure that those operations respect the principle of non-refoulement.
- The General Court had erred in considering that Frontex provided only technical and operational support to Member States, without being obliged to verify whether there was a return decision.
- The General Court had also erred in finding that any infringements of fundamental rights occurring during a return flight fall within the sole responsibility of the host Member State, to the exclusion of any responsibility on the part of Frontex.

The ECJ therefore set aside, in large part, the judgment under appeal taking into account Frontex's obligations in connection with the protection of the fundamental rights of persons included in joint return operations.

➤ *The pushback case*

Regarding the alleged pushback, the ECJ found that the General Court had infringed the applicant's right to effective judicial protection by not correctly applying the rules on the burden of proof and the taking of evidence:

- The ECJ recalled that Frontex is legally responsible for activities which it oversees or coordinates. During those activities, Frontex must ensure respect for fundamental rights and the principle of non-refoulement.
- The right to an effective remedy, as guaranteed by Art. 47 of the EU Charter of Fundamental Rights, would be illusory if victims of a pushback in a zone in which Frontex was conducting operations were required to demonstrate, by way of conclusive proof, that that pushback had occurred and that they had been present at it. Frontex, however, is likely to possess information making it possible to prove the existence of pushbacks, given its task of collecting operational data and its obligation to ensure respect for fundamental rights during its operations.
- Consequently, the ECJ found that the right to effective judicial protection requires an adaptation of the burden of proof, such that a person who claims to be a victim of a pushback involving Frontex need not produce conclusive proof but rather sufficiently detailed, specific, and consistent *prima facie* evidence that that pushback occurred and that he/she was present at it.

The ECJ stated that, if such *prima facie* evidence is produced, the General Court is required to investigate the case in order to be able to assess the truth of said pushback and of the applicant's presence at it.

➤ *Put in focus*

The ECJ's two rulings in *WS* and *Hamoudi* are likely to send a strong signal. They take account of the changing role of Frontex, meaning that the EU border and coast guard agency can no longer be viewed merely as a technical support unit, but must actively ensure that fundamental rights are upheld. (CR)

Frontex Report on Earth Observation for Border Management

At the beginning of December 2025, Frontex published a new report examining how Earth Observation (EO) technologies can support national authorities managing the EU's external borders. The report entitled "Earth Observation for Border Management" explores where satellite and airborne data add the greatest value for border surveillance, where gaps remain, and which trends will shape future capabilities. It sets out how EO can be used to address border-related challenges, such as detecting illegal border crossings and smuggling activities, as well as supporting humanitarian operations, such as search and rescue.

The report explains the main EO technologies and platforms used in border monitoring, including different sensors and satellite systems, outlining their key characteristics, typical resolutions, technical strengths, and principal border management applications.

It also presents six border surveillance use cases for maritime border surveillance:

- Vessel detection and tracking;
- Coastal and pre-frontier monitoring;
- Cross-border crime monitoring;
- Land border surveillance;
- Monitoring of irregular migration.

For each of these six areas, the currently deployed technologies are described alongside identified gaps and limitations, supported by a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis.

Looking at cross-border crime monitoring, the report highlights how EO technologies significantly enhance situational awareness by providing high-resolution, all-weather surveillance across vast and remote areas. Satellite imagery is increasingly used by authorities to detect and disrupt cross-border criminal activity, offering both operational and evidentiary value relevant to legal practice. High-resolution images can reveal land-based smuggling routes through indicators such as newly created dirt roads, trails, fence breaches, or vehicle concentrations. EO technologies also support the detection of illicit crops and criminal sites, with multispectral, thermal, and hyperspectral data enabling the identification of illegal cultivation, hidden drug laboratories, or chemical traces linked to organized crime.

In the maritime domain, satellite radar and optical imagery have enabled major operations, including Frontex-coordinated operations resulting in the seizure of narcotics and large

volumes of smuggled cigarettes. Satellite surveillance further supports border security in conflict- or terrorism-affected regions by monitoring troop movements, militant infiltration, and infrastructure changes. While the detection of underground tunnels remains technically challenging, repeated imagery can reveal surface disturbances indicative of tunnelling or fortification activities, thereby strengthening intelligence and enforcement actions.

In its final chapter, the report sets out the challenges in EO-based border management:

- Coverage versus persistence: While satellites provide wide-area coverage, current constellations do not offer continuous monitoring of any single location;
- Weather and lighting constraints;
- Resolution and identification limits;
- Data overload and analysis bottlenecks;
- Integration and interoperability challenges;
- Adversary countermeasures: Smugglers and migrants may use camouflage, operate during cloud cover or new-moon periods, deploy decoys, or exploit predictable surveillance patterns. There have also been instances of spoofing or the deliberate deactivation of tracking devices, and, in extreme cases, interference with navigation systems;
- Costs and accessibility;
- Privacy and ethical concerns: Balancing border security objectives with fundamental rights remains complex when authorities must ensure that EO data is used strictly for legitimate law-enforcement purposes and not for indiscriminate surveillance.

The EO report contributes to the Copernicus Border Surveillance Service (CBSS), where Frontex was entrusted to explore how space-based data can support EU Member States in tackling irregular migration and cross-border crime. (CR)

Areas of Crime

Protection of Financial Interests

ECA: EU Anti-Fraud Bodies Could Do Better

spot light

On 15 December 2025, the European Court of Auditors (ECA) tabled a special report assessing on how the EU's primary anti-fraud bodies, i.e., the EPPO, OLAF, Eurojust and Europol, cooperate in investigating fraud against the EU budget. The audit examined the following:

- The clarity and comprehensiveness of the four EU bodies' mandates, roles and responsibilities for investigating fraud as well as their mutual support during the investigation lifecycle;
- The procedures for handling allegations of fraud, particularly with a view to avoiding duplication and inefficiency and ensuring a regular information flow;
- The mechanisms used by the Commission to oversee fraud detection activities and to ensure due compensation for the EU budget.

The audit was designed to provide an input into the Commission's White Paper on the review of the EU's anti-fraud architecture (→eucrim 2–2025, 137–138). Overall, the ECA found that, while the bodies' responsibilities are clearly defined, weaknesses remain in terms of the exchange of information, which affects the number and timeliness of the EPPO's and OLAF's investigations. Shortcomings also arose with regard to the Commission's mechanism for monitoring whether the recoveries ordered by national courts have taken place and whether the full amount due to the EU budget has been recovered. Other key conclusions of the report regarding the aforementioned three areas of scrutiny include the following:

➤ *The bodies' mandates*

- The roles and responsibilities of OLAF, the EPPO, Europol and Eurojust are clear and do not overlap. This gives them the potential to effectively protect against fraud affecting the EU's financial interests;
- Collaboration: the number of cases in which the bodies supported one another has remained relatively small in recent years, compared to the number of investigations opened by both the EPPO and OLAF. One possible reason for this is that the EPPO's primary source of support is national authorities, and that OLAF's administrative remit differs substantially from that of the other three EU bodies.

➤ *The procedure of handling fraud allegations*

- The current dual reporting system is cumbersome and leads to duplication of investigative work on the part of the EPPO and OLAF;
- There is limited information exchange from the EPPO to OLAF regarding the state of play of investigations, e.g. discontinuation or indictments – this limits the scope for further protective measures.

➤ *The Commission's oversight mechanism*

- There is no clear picture of the adequacy of the level of fraud detection by the EPPO and OLAF;
- The Commission has no adequate mechanism to show the recovery results from criminal or administrative procedures.

In light of these findings, the ECA made three key recommendations to the Commission:

- By the end of 2028, establish an interoperable anti-fraud system (based on specific proposed principles) that clarifies where fraud allegations should be reported, and facilitate an efficient exchange of information on fraud allegations and investigations;
- By the end of 2026, analyse the variations in fraud reporting across the EU and take appropriate action, such as investigating causes of significant under-reporting;
- By the end of 2028, enhance oversight of the follow-up of fraud investi-

gations by developing a methodology to measure the overall financial impact of EPPO and OLAF investigations, and by requiring Member States to regularly report asset conversion and recovery amounts.

The ECA's special report (No 26/2025), a factsheet on the key findings, and the replies to the report from the Commission, the EPPO, and Europol are available on a dedicated website. (TW)

Conditionality Mechanism: Slovak Whistle-Blower Legislation Sparks Concerns at EPPO

On 16 December 2025, the European Chief Prosecutor addressed a letter to the European Commission expressing concerns over amendments to the Slovak law on whistle-blower protection. The amendments had just been proposed by the government of the Slovak Republic and were scheduled to be adopted one week later under an expedited legislative procedure.

Following an analysis of the draft legislation, the European Chief Prosecutor concluded that it contains several elements that cannot be reconciled with the principles of the rule of law as set out in Regulation (EU) 2020/2092 of 16 December 2020 on a general regime of conditionality for the protection of the budget of the European Union.

In particular, the proposed amendments would restrict whistle-blower protection for certain categories of persons, notably those who are not directly employed by the entity whose alleged misconduct is reported. The letter states that a failure to ensure adequate protection for all whistle-blowers, including members of police forces, would significantly limit the detection, reporting, and investigation of corruption. The proposal would also introduce the retroactive application of the amendments, which, if adopted, would directly affect ongoing cases handled by EPPO. Therefore, the European Chief Prosecutor informed the European Commission in accordance with Recital 16 of Regulation (EU) 2020/2092 that, should the amendments be adopted, they would have a negative impact on the efficiency of criminal investigations into breaches of the law in general and on the overall level of protection of the financial interests of the EU. (CR)

EP Calls for Improvements to Conditionality Regulation

spot light

On 18 December 2025, the plenary session of the European Parliament adopted a resolution on the implementation of the rule of law conditionality regime. Five years after the Regulation on a general regime of conditionality for the protection of the EU budget (the "Conditionality Regulation", →eucrim 3/2020, 174–176) came into force, the EP resolution takes stock and draws attention to deficiencies in its implementation. The Conditionality Regulation allows the EU to suspend or reduce funds if rule-of-law breaches pose a direct risk to the EU budget or the EU's financial interests. Key issues raised by the resolution include:

- The Commission must react in a timely manner, in order to ensure a more effective protection of the EU's financial interests;
- The Commission's assessment of rule-of-law breaches lack transparency as it either fails to produce proposed measures or results in the selection of an alternative instrument;
- The Commission should accept complaints in any written form and establish a confidential reporting portal to protect whistleblowers;
- Political deadlock or blackmail used by concerned Member States to obstruct EU decision-making must be rejected;
- The systemic and persistent nature of the breaches of the rule of law by the Hungarian government should lead to a much larger proportion of EU funding being suspended (up to 100% of all funding instead of 55% for specific programmes as applied);
- The relationship between the Conditionality Regulation and other instruments in the rule of law toolbox is unclear, particularly with regard to the horizontal enabling condition on the CFR under the Common Provisions Regulation and the rule of law super milestones under the Recovery and Resilience Facility (RRF), which undermines trust in the unbiased application of the Conditionality Regulation.

MEPs also reiterated their request for the EP and civil society organisations to play a stronger role in the application of the conditionality regime, including better information sharing.

The resolution sets out a series of recommendations aiming at improving the effectiveness and transparency of the Conditionality Regulation, as well as its coordination and consistency with other instruments in the rule of law toolbox. Recommendations include revising the 2022 guidelines (→eucrim 1/2022, 22–23), making more proactive use of the Regulation, and strengthening safeguards for the final recipients and beneficiaries. It also advocates a closer integration of the conditionality mechanism with the Commission's annual rule of law reports.

Lastly, the EP calls for a unified, coherent, and comprehensive framework to be established across all EU funding programmes in the 2028–2034 MFF. In this context, all rule of law tools should be consolidated into a single framework. (TW)

Money Laundering

Cryptocurrency Fraud Infrastructure Dismantled

A large-scale international law enforcement operation, executed in two coordinated phases in October and November 2025, has dismantled the core infrastructure of a cryptocurrency

fraud and money-laundering network that processed more than €700 million in illicit funds. The operation was supported and coordinated at the EU level by Europol and Eurojust. What began as an investigation against a single cryptocurrency platform evolved into the exposure and takedown of an interconnected criminal ecosystem operating across Europe and beyond. Raids, arrests, and seizures were carried out across Belgium, France, Germany, Spain, Cyprus, Malta, Bulgaria, and Israel.

The operation targeted and dismantled three critical pillars of the fraud infrastructure:

- Authorities shut down fraudulent cryptocurrency investment platforms and associated call-centre operations that used social engineering to extract funds from victims;
- The network's financial laundering infrastructure was disrupted through coordinated seizures of bank accounts, cryptocurrency wallets, cash, and digital devices used to obscure illicit flows across blockchains and exchanges;
- Investigators neutralised the affiliate marketing and online advertising infrastructure that generated victims at scale, including companies behind deceptive social media campaigns using impersonation and deepfake content.

The operation resulted in multiple arrests and seizures, including bank accounts worth €800,000 and €415,000 in cryptocurrencies. Law enforcement authorities will continue to track the criminal organisation's assets in the countries where it has operated. (CR)

"Cryptomixer" Taken Down

At the end of November 2025, Europol and Eurojust helped German and Swiss authorities during a coordinated action week in Zurich that led to the takedown of the illegal cryptocurrency mixing service "Cryptomixer". The service is suspected of having facilitated cybercrime and money laundering since 2016. It has allegedly enabled the laundering of over €1.3 billion in Bitcoin by obscuring transaction trails linked to offences including ransomware attacks, drug and weapons trafficking, and payment card fraud.

As key domains were located in Germany and servers in Switzerland, authorities from both countries collaborated closely to conduct investigations and take action against the service. A joint investigation team was established at Eurojust to enable real-time exchange of information and evidence. Europol provided operational coordination, intelligence exchange through the Joint Cybercrime Action Taskforce (J-CAT), and on-the-spot forensic support.

During the action days, law enforcement seized three servers, the *cryptomixer.io* domain, over 12 terabytes of data, and more than €25 million in cryptocurrencies. A seizure notice was placed on the website. (CR)

Dutch Organisation Calls for Improved Safeguards When Implementing New EU AML Package

In a consultancy paper for the Dutch government, the Dutch non-governmental organisation Privacy First called for robust safeguards to be implemented alongside the new EU's anti-money laundering legislation (→eucrim 2/2024, 113 et seq.). In light of the planned implementation of the AML/CFT package in the Netherlands, Privacy First is particularly concerned about the involvement of private companies ("obliged entities") in the fight against money laundering and terrorist financing, in particular:

- Assigning unsuitable tasks to companies;
- The disproportionate costs incurred by obliged entities that are passed on to customers;
- The failure to respect the fundamental rights of citizens, and small and medium-sized enterprises (SMEs) and non-profit organisations.

According to Privacy First, safeguards must be improved during the implementation of the EU regulations. These include:

- Improved legal protection of consumers, SMEs, and non-profit organisations, including through the establishment of a financial ombudsman to handle all anti-money laundering complaints and low-threshold access to the independent courts;
- A secure channel for obliged entities to communicate about their customer due diligence;
- The inclusion of a requirement for any automated customer risk profiling to follow the principles of the EU AI Act, including a fundamental rights compliance assessment;
- An obligation for anti-money laundering supervisors, such as the Dutch central bank, to enforce compliance by obliged entities with data protection rules and respect for customers' fundamental rights;
- Periodic mandatory audits by independent auditors on compliance to ensure public authorities and larger obliged entities comply with data protection and fundamental rights legislation.

Through its paper, Privacy First also seeks to spark a public discussion on the privatisation of crime fighting, and calls on politicians to adjust rules, which provide inadequate protection for fundamental rights. (TW)

Counterfeiting & Piracy

Outcomes of Operation LUDUS

On 27 November 2025, Europol, OLAF and the European Union Intellectual Property Office (EUIPO) announced the results of the law enforcement operation LUDUS V. LUDUS is an annual law enforcement operation that focuses on preventing the distribution of fake and unsafe toys in the EU market (for previous editions →eucrim 2/2023, 122; →eucrim 1/2022, 28;→eucrim 1/2021, 13).

The fifth edition of the operation that was carried out between 2024 and 2025 resulted in the coordinated seizure of 4.2 million counterfeit toys infringing intellectual property rights and 3.6 million unsafe toys posing potential safety hazards. 86 persons were reported to judicial authorities.

OLAF coordinated actions of customs authorities in 13 EU Member States and involved rights holders that contributed to the success of the operation.

The EUIPO provided logistical support and facilitated collaboration between rights holders from the private sector and enforcement authorities through the Intellectual Property Enforcement Portal (IPEP).

Europol played a major role in planning the various phases of the operation.

With regard to operation LUDUS IV (carried out between 2023 and 2024), OLAF reported that around 500,000 toys were seized, including dolls, plush toys, board games, and video game consoles. The value of the seized goods was estimated at €2 million.

The information about the results of operations LUDUS V and IV comes along with a separate Europol report, which provides an overview of the outcomes of the LUDUS iterations over the last five years (2020–2025). According to the report entitled "Cheating the Toy World", the five editions of LUDUS achieved the following operational results:

- Nearly 50 million illicit toys, valued at almost €150 million were seized;
- Nearly 27,700 law enforcement inspections were carried out;
- 417 individuals were reported to judicial authorities and 31 were arrested;
- Between 18 and 29 countries have engaged in the enforcement actions.

Europol emphasised that counterfeiters profit from the high demand for low-priced toys. Major trends observed during the LUDUS operations include:

- Counterfeiters often operate from outside the EU, which poses a challenge to EU law enforcement efforts;
- Crimes are predominantly facilitated by online commerce, whereby commerce via social media platforms have become a primary channel for counterfeiters to advertise illicit toys;
- Perpetrators mainly exploit the digitalisation of society and technological innovations, such as 3D printing and AI-driven marketing;
- Social commerce and small parcel distribution continue to pose significant challenges to detection and traceability.

Europol concluded that EU law enforcement will continue to prioritise the fight against the dangerous trade in counterfeit toys and the criminal actors behind it. Sustained operational activity, targeted monitoring and effective intelligence sharing among stakeholders remain essential to prevent and detect IP crime. (TW)

"Pirates 3" Targets Border Smuggling

On 12 December 2025, Frontex informed the public about the Joint Action Days "Pirates 3": a large-scale, intelligence-led operation conducted at the EU's external borders, targeting organised criminal networks smuggling people and illicit goods. The operation took place between 6 and 17 October 2025; Frontex, Europol, and the European Union Intellectual Property Office (EUIPO) supported national law enforcement authorities from more than 10 countries.

The coordinated action resulted in the detection of 64 cases of irregular border crossings and the seizure of 261 falsified or fraudulent travel and identity documents, including passports, ID cards, residence permits, and driving licences. Authorities also intercepted more than 420,000 counterfeit items spanning textiles, footwear, cosmetics, electronics, toys, and automotive parts.

The numbers underscore the continued scale of cross-border IP infringement: Significant excise and financial crime outcomes were recorded, with over 17.5 million cigarettes and 6500 e-cigarettes seized, alongside €1.156 million in undeclared cash. Enforcement activity was further extended to narcotics and weapons trafficking, resulting in the seizure of 1,698kg of marijuana, 1.2kg of methamphetamine, 148 pistols, 179 magazines, and 122 cartridges. Additional undeclared goods included pharmaceutical products, luxury watches, and foodstuffs.

The Joint Action Days "Pirates 3" took place within the framework of EMPACT — the European Multidisciplinary Platform Against Criminal Threats. It prioritises the fight against the most important threats posed by serious and organised international crime affecting the EU (→eucrim 2/2025, 142). (CR)

Organised Crime

Fight against Drugs: Commission Presents New Drugs Strategy and New Legislation against Precursors

spot light

On 4 December 2025, the European Commission presented a new EU Drugs Strategy together with an Action Plan against drug trafficking and a proposal to revise the rules on drug precursors. The initiatives form part of the ProtectEU – European Internal Security Strategy (→eucrim 1/2025, 3–4) and set out a comprehensive response to the security, health, social, and environmental challenges linked to illicit drugs.

The new EU Drugs Strategy is structured around five priority areas:

- Strengthen preparedness and threat response through improved data collection, monitoring, and early warning systems, with a reinforced role for the EU Drugs Agency (EUDA);
- Enhance public health protection by supporting prevention, treatment, and reintegration measures;
- Advance security-oriented measures, including upcoming proposals to

tighten rules against organised crime and an evaluation of the Framework Decision on drug trafficking by 2026; other measures in this pillar include strengthening public-private cooperation to improve the detection of drugs in postal and parcel services as well as the development of a new EU Ports Strategy;

- Prevent drug-related harm, with a focus on measures to protect young people from recruitment into organised crime;
- Build stronger partnerships to address the drug situation, in particular by reinforcing and expanding international alliances with third countries and regions.

The accompanying EU Action Plan against drug trafficking has translated these objectives into operational measures across six areas, including:

- Adapting to evolving trafficking routes and modi operandi used by criminal networks;
- Preventing crime and drug-related violence;
- Enhancing cooperation between law enforcement and judicial and customs authorities, with Europol at the centre of supporting drug trafficking online;
- Tackling synthetic drugs and precursors;
- Promoting research and innovation, with a new Security and Innovation Campus to be launched in 2026;
- Strengthening international cooperation, in particular by joint investigations between the law enforcement authorities of EU Member States and partner third countries, and fostering ports resilience.

In parallel, the Commission proposed updated rules on drug precursors and so-called designer precursors. The proposal for a respective Regulation (COM(2026) 747 final) introduces real-time reporting of significant seizures, faster procedures to control emerging substances, and a ban on certain designer precursors. It also aims to simplify and digitalise procedures for legitimate operators to reduce administrative burdens. The proposal will replace existing EU regulations on precursor trade and forms a key part of the EU Drugs Strategy, enhancing law enforcement and customs capacities to disrupt drug production networks.

When presenting the new EU Drugs Strategy, *Magnus Brunner*, Commissioner for Internal Affairs and Migration, said: "[T]his integrated European response focused on readiness and prevention aims to deliver sustainable solutions crucial to protect our social fabric and set global standards for our partners." (AP)

Denmark Summarises EU Fight against Drug Trafficking

The Danish Council Presidency compiled a report that summarises the actions taken in view of the 2023 EU Roadmap to fight drug trafficking and organised crime (→eucrim 3/2023, 257). The rolling out of the roadmap came to an end in December 2025. The summary relates to the main priority areas which were defined in the roadmap and which served as the basis for Member States' actions during the Belgian, Hungarian, Polish and Danish presidencies. These include:

- Mobilisation of the customs community against drug trafficking;
- Strengthened law enforcement operations in ports;
- Improved public-private partnership against drug smuggling and criminal infiltration;
- Mapping the most threatening criminal networks;
- Facilitation of financial investigations;
- Facilitation of digital investigations.

It is concluded that the trio Council Presidencies (Poland, Denmark and Cyprus) have closely cooperated in furthering tangible progress in dismantling serious organised drug trafficking networks and preventing additional drug-related harm to EU citizens and society as a whole. The Presidencies will also support the Commission new EU Drug Strategy which was presented on 3 December 2025 (→previous news item). (TW)

Trafficking in Human Beings

Joint Declaration on Global Alliance to Counter Migrant Smuggling

At the second conference of the Global Alliance to Counter Migrant Smuggling, held in Brussels on 10 December 2025, delegations from EU Member States and partner countries, as well as international organisations, adopted a joint declaration reaffirming their common commitment to strengthening international cooperation against migrant smuggling. The declaration is based on three pillars:

- Prevention;
- Response;
- Development of alternatives.

With regard to prevention, the delegations committed, *inter alia*, to supporting awareness-raising campaigns to counter the narratives of smugglers and to enhancing collaboration with transport operators, authorities, and stakeholders to counter the use of commercial transport for irregular migration, such as in air transport.

A series of measures were agreed upon to more effectively respond to migrant smuggling, e.g.:

- Strengthened operational cooperation along migratory routes at all levels;
- Intensified cooperation with digital platforms to curb smugglers' increased use of digital tools;
- Improved financial investigations to trace, seize, and confiscate smuggling proceeds and dismantle the economic infrastructure of smuggling networks;
- Combat corruption and fraud facilitating migrant smuggling;
- Stepping up efforts for capacity-building, technical assistance, and peer-to-peer cooperation.

Finally, the EU and its partners reaffirmed their committments to showing victims that there are safer alternatives to illegal migration. Support measures, such as better vocational education and training, will be implemented in both countries of origin and destination.

The Global Alliance to Counter Migrant Smuggling was launched in 2023 on the initiative of the European Union and has achieved significant results in disrupting smuggling operations and strengthening international cooperation. Main achievements since 2023 include:

- A €700 million investment for the prevention of migrant smuggling and trafficking in human beings;
- The establishement of a network of digital-investigation experts;
- A stronger Europol mandate with additional €50 million and 50 staff to boost action against smuggling and trafficking in human beings;
- Joint law enforcement projects with partner countries in Europe, Africa and Asia to dismantle trafficking networks.

In the future, another €128.9 million will be allocated for actions across the Western Balkans, Africa, Asia and Latin America by the end of 2026. (TW)

THB and Labour Exploitation: Key Study Findings

In December 2025, the EU Anti-Trafficking Hub published a new study examining trafficking in human beings (THB) for the purpose of labour exploitation, drawing on examples from Italy, Finland, France, Spain, and the Netherlands. The study analyses how THB for labour exploitation is addressed across national systems, highlighting the complexity of existing legal frameworks and the persistent challenges in distinguishing trafficking from other forms of labour exploitation.

The publication is structured into four main sections:

- Section 1 introduces the phenomenon of trafficking for labour exploitation, presents the "continuum of exploitation" as a guiding conceptual framework, and outlines relevant EU and international definitions. It also gives an overview of national legislation in the selected Member States.
- Section 2 examines how different legal concepts are interpreted and applied in practice, with a particular focus on national case law.
- Section 3 identifies regulatory and practical gaps and challenges, while also highlighting national approaches, tools, and promising practices.
- Section 4 sets out concrete recommendations to strengthen legal and institutional responses to trafficking for labour exploitation.

The concept of a "continuum of exploitation," which situates human trafficking alongside forced labour and other forms of severe labour abuse within EU and international legal frameworks, is central to the analysis. This approach recognises labour exploitation as a spectrum of harmful practices that may evolve over time and encompass acts of differing severity, manifested through varying degrees of vulnerability, dependency, and coercion. However, operationalising this perspective remains challenging, particularly within criminal justice systems designed to address single offences rather than evolving patterns of exploitation. As a result, depending on national legislation, situations of labour exploitation may fall under administrative, labour law, or criminal justice mechanisms. The absence of specific criminalisation of serious labour exploitation in many Member States, combined with limited awareness among practitioners, further complicates effective identification and response. Against this background, the report explores the use of complementary criminal and administrative offences as alternative enforcement tools and reviews national practices, including the role of labour inspectors, specialised authorities, and national action plans.

The study concludes with targeted recommendations:

- Strengthening the use of the EU Anti-Trafficking Directive;
- Developing national guidelines and common trafficking indicators;
- Proactively initiating investigations where indicators are present;
- Ensuring access to comprehensive victim support and remedies;
- Investing in specialised investigators, prosecutors, and judges with expertise in labour exploitation cases.

The publication complements recent work by the EU Agency for Fundamental Rights (FRA) and the European Labour Authority (ELA), which jointly released a practical guide and training manual to support labour inspectors in identifying and addressing labour exploitation in the workplace (→eucrim 3/2025, 206–207). (CR)

Procedural Law

Data Protection

Council Gives Input for Review of Data Protection Directive

At the end of November, the Council adopted its position on the evaluation and review of Directive 2016/680 on data protection in the law enforcement area (commonly known as "LED"). The Council's document shares observations from the EU Member States in the application of the LED. It provides input for the European Commission which is due to submit an evaluation report in 2026.

The Council finds that the introduction of the Directive has had and continues to have a significant impact on awareness, accountability and compliance, and has further increased the security of data processing among

competent authorities. The Council sees, however, several issues that need to be further implemented in the future, including:

- Take proactive steps for more adequacy decisions (so far only one with the UK exists) in order to facilitate data transfers with non-EU countries;
- Clarify legal questions that have arisen and will arise with regard to the interplay between the AI Act and the LED;
- Obtain more clarity on specific issues that came to light as a result of national implementation.

The Council voices its general satisfaction with the application of the data subjects' rights enshrined in the LED, in particular with the most commonly exercised rights of access and erasure. However, difficulties emerge in practice if these data subjects' rights overlap or intersect with other rules and procedures regarding access to documents or confidentiality, or with general rules or principles of criminal procedure under national law. The Council encourages the EDPB to work on guidance in this respect taking into account the needs of competent authorities. In addition, further guidance is needed with regard to the alleviation of administrative burdens, e.g. burdens associated with access requests. (TW)

Commission Renewed Adequacy Decisions for Data Transfers to the UK

On 19 December 2025, the European Commission reaffirmed that the United Kingdom (UK) ensures an adequate level of data protection so that personal data can continue to be transferred to the UK as third country. The Commission adopted two adequacy decisions: one based on the General Data Protection Regulation (GDPR) and one based on Directive 2016/680 (the "Law Enforcement Directive", LED).

Regarding data transfers for criminal law enforcement purposes, the Commission decision was taken on the basis of Art. 36 LED, which protects personal data that is used by police and criminal justice authorities. This decision permits data transfers from law enforcement authorities of the EU Member States to UK law enforcement authorities without the need for further authorisation.

It follows the Commission's previous adequacy decision, taken in 2021, and an interim extension endorsed in June 2025, as the 2021 adequacy decisions would have expired on 27 June 2025, and the Commission needed time to review the UK's latest legislative reforms by the Data (Use and Access) Act. The renewal also takes into account an opinion by the European Data Protection Board (adopted on 16 October 2025) and comes after the Member States had given green light in the so-called comitology procedure. The adequacy decision is also binding on EU countries with opt-out/opt-in reservations in justice and home affairs (i.e., Ireland and Denmark) and on the Schengen associated countries (Iceland, Norway, Liechtenstein and Switzerland).

The adequacy decision is subject to a "sunset clause", as it will expire on 27 December 2031 unless it is extended. According to the LED, the Commission is obliged to monitor relevant developments in the UK on an ongoing basis in order to assess whether the UK still ensures an essentially equivalent level of protection. This is particularly important given that the UK will apply and enforce a modified data protection regime, with further secondary legislation potentially changing the data protection framework. In addition, a periodic review is required at least four years

Procedural Safeguards

ERA: Free EU Criminal Law Training Resources for Defence Lawyers

The Academy of European Law (ERA), together with partners, has released a set of free training materials aimed at strengthening defence lawyers' capacity to handle cross-border criminal cases across Europe. The resources are openly accessible online and are part of the "European Criminal Law for Defence Lawyers" project. The programme "European Criminal Law for Defence Lawyers" focuses on practical understanding of EU tools, such as the European Arrest Warrant and the European Investigation Order, as well as broader procedural rights and rule-of-law safeguards.

The initiative is co-financed by the European Commission under EU justice funding programmes, supporting a two-year training effort that includes seminars, webinars, e-learning modules, and publicly available materials. The materials are designed to address the growing number of cross-border criminal proceedings, where knowledge of national law alone may be insufficient. The training package includes:

- Background documentation on EU criminal law topics;
- Self-paced e-learning modules;
- Recorded webinars and video lectures.

Subjects covered range from mutual recognition instruments and legal privilege to digitalisation in criminal justice, including e-evidence and video-conferencing. The modules also explain the roles of EU agencies involved in criminal cooperation, including Europol, Eurojust, and the European Public Prosecutor's Office.

The project reflects broader EU efforts to enhance mutual trust and consistent application of European criminal law through practitioner training and cooperation. (CR)

after the adoption of the adequacy decision. This review must evaluate the functioning of the adequacy decision, including the functioning of the relevant oversight and enforcement mechanisms in the UK.

Likewise, the Commission renewed its adequacy decision under Art. 45 of the GDPR. This ensures that personal data can continue to flow freely and safely between the European Economic Area (EEA) and the UK for the purposes covered by the GDPR. The Commission has clarified that the scope of the renewed adequacy decision now also covers the transfer of personal data for UK immigration control purposes. An "immigration exemption" was included in the 2021 adequacy decision for GDPR-related purposes.

Michael McGrath, Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, said: "The United Kingdom is an important strategic partner for the European Union and the adequacy decisions form a central pillar of this partnership. By enabling the free flow of personal data, they underpin both commercial exchanges and cooperation in the fields of justice and law enforcement." (TW)

EU Council Moves Ahead on Data Sharing for US Border Purposes

On 16 December 2025, the Council adopted a Decision formally opening the way for negotiations on a comprehensive framework agreement between the EU and the United States of America on the exchange of information for security screenings and identity verifications related to border procedures and visa applications. The Decision followed the respective Recommendation for such Council Decision tabled by the European Commission on 23 July 2025.

➤ *The EU's approach*

The main parameters for the future agreement are set out as follows:

- The reciprocal exchange of information to assess whether travellers pose a risk to public security or public order. Any subsequent use of exchanged data for purposes such as addressing irregular migration or preventing, detecting, and combating serious crime or terrorism is only allowed where it is strictly necessary, duly authorised, and carried out within existing legal frameworks.
- The framework agreement must fully respect fundamental rights and comply with EU data protection rules, including the General Data Protection Regulation, the Law Enforcement Directive, and other relevant EU legislation, notably the Artificial Intelligence Act.
- The agreement will not replace or affect existing EU–US cooperation instruments in the fields of law enforcement and criminal justice, including agreements on the prevention and combating of serious crime (PCSC) and mutual legal assistance (MLA). Member States may conclude bilateral arrangements with the United States on matters covered by the framework agreement, provided that such arrangements are compatible with EU law.

In line with existing treaty opt-outs, Denmark and Ireland are not taking part.

The framework agreement is necessitated because the US changed the requirements for its Visa Waiver Program. Accordingly, countries are required to conclude an "Enhanced Border Security Partnership" (EBSP) with the U.S. Department of Homeland Security.

➤ *The EDPS Opinion*

The European Data Protection Supervisor (EDPS) provided an opinion on the planned deal on 17 September 2025. He noted that the proposed framework agreement would set an important precedent, as it would be the first EU agreement involving large-scale sharing of personal data, including biometric data, for border and immigration control purposes by a third country. He therefore stressed the need to ensure that any data processing remain strictly necessary and proportionate.

While generally supporting the establishment of a common EU–US framework with Union-level safeguards, the EDPS called on the Commission and the Council to take into account a number of specific recommendations, including the following:

- Fundamental rights impact assessment: Conduct an in-depth fundamental rights impact assessment of both the proposed framework agreement and the Enhanced Border Security Partnerships with the United States. The level of interference with individual rights should be considered comparable to that of data exchanges for law enforcement purposes.
- Narrow and clearly defined scope: Define the personal scope of the framework agreement exhaustively and narrowly, taking into account existing prohibitions on data sharing under EU law.
- Strict limits on data categories: Clearly and comprehensively circumscribe the categories of personal data that may be exchanged, including any supplementary information provided to US authorities.
- Protection of EU large-scale IT systems: Explicitly exclude any direct or indirect sharing or transfer of data from EU large-scale IT systems in the area of justice and home affairs, in particular those related to migration and asylum.
- Strong accountability and transparency safeguards: Ensure clear and specific justification for each data query, robust accountability mechanisms, and transparency obligations for both EU and US authorities.
- Safeguards for Member States and individuals: Provide a legal possibility for Member States to refuse data sharing in individual cases and ensure access to effective judicial redress in the USA, regardless of an individual's

citizenship or the purpose of the data processing.

➤ *Further criticism*

The plan for the framework agreement in the context of the EBSP also met criticism in media and by civil society organisations. As Euractiv reported, the EU institutions involved seem to have nearly no reservations to share personal data with the US, including sensitive data of EU citizens. Concerns have also been raised regarding the possibility that EU Member States can engage in direct talks with the US administration to conclude their own agreements within the EU framework. Recent events, such as the sanctioning by the US administration of Commission officials and EU citizens involved in lawmaking and advocacy work, have further fueled these concerns.

Statewatch criticised that the agreement would massively expand data-sharing via US access to EU Member State's law enforcement databases and go beyond what is necessary under the Visa-Waiver Program. It also stated that it is quite unclear how the Commission would ensure that the EU data protection safeguards are built in. "US privacy law ostensibly designed to provide redress to Europeans was already insufficient, even before the Trump administration's ongoing demolition of privacy and data protection standards – not to mention the broader erasure of the rule of law within the US", Statewatch said. (CR)

New Regulation Speeds Up Handling of Cross-Border GDPR Complaints

On 26 November 2025, the European Parliament and the Council finally adopted a new Regulation laying down additional procedural rules on the enforcement of the General Data Protection Regulation (GDPR). The Regulation (Regulation 2026/2518) was published in the Official Journal L, 2025/2518 of 12.12.2025. It will improve cooperation between national data protection authorities in enforcing the GDPR. The law seeks to streamline how cross-border data protection complaints are handled across the EU, making procedures more efficient and predictable.

Under the new rules, the criteria for determining whether a cross-border complaint is admissible have been harmonised so that admissibility is assessed on the same basis – regardless of where a complaint is filed. Common procedural safeguards have also been introduced, including clear rights for complainants and organisations under investigation to be heard and to see preliminary findings. For straightforward cases, data protection authorities will have the option to use a simplified cooperation procedure without invoking the full set of cooperation mechanisms. The Regulation also imposes time limits: regular investigations are expected to conclude within 15 months, with possible extensions for complex cases, and simpler procedures within 12 months.

Regulation 2025/2518 entered into force on 1 January 2026 and it will apply from 2 April 2027. (AP)

ECJ: Indiscriminate Collection and Unlimited Storage of Biometric and Genetic Data Permissible

spot light

On 20 November 2025, the European Court of Justice (ECJ) ruled in case C-57/23 ("*JH v Policejní prezidium*") that the indiscriminate collection and indefinite storage of biometric and genetic data of individuals is permissible, provided that there is a strict necessity and regular review is guaranteed.

➤ *Background of the case and questions referred*

The ruling was prompted by Czech proceedings in which a suspect took action against identification measures and their storage by the Czech police. Paragraph 65 of the Law on the Czech Police stipulates, *inter alia*, that the police may, for the purpose of future identification of a person accused or suspected of having committed an intentional criminal offence, take fingerprints, identify physical features, perform body measurements, obtain visual, audio, and similar recordings, and take biological samples that make it possible to obtain information about his or her genetic make-up. The police subsequently record that information in the relevant databases.

The Nejvyšší správní soud (Supreme Administrative Court of the Czech Republic) had doubts as to whether this legal regime is compatible with Directive 2016/680, which protects individuals with regard to the processing of their personal data by police and criminal justice authorities ("Law Enforcement Directive", LED). Two issues were mainly put forward:

- Do the requirements laid down in Directive 2016/680 preclude the indiscriminate collection of biometric and genetic data in respect of any person suspected of having committed an intentional criminal offence?
- Do the requirements laid down in Directive 2016/680 preclude the storage of biometric and genetic data without a maximum time limit?

➤ *The ECJ's reasoning on the indiscriminate collection of biometric/genetic data*

Regarding the question on whether Directive 2016/680 precludes national legislation which permits the indiscriminate collection of biometric and genetic data of any person accused or suspected of having committed an intentional criminal offence, the ECJ first clarified that Art. 6 LED does not oblige Member States to make a distinction between "persons accused" and "persons suspected" of having committed an intentional criminal offence. However, data controllers are required, in accordance with national law, including the case-law of the national courts, to comply with all of the principles and specific requirements laid down in Arts. 4 and 10 LED. In particular, this means that the processing

must be "strictly necessary". This concept includes, *inter alia*:

- The "purpose of the processing" must refer to the specific and real aims pursued by the processing of personal data in the light of the task of the controller in the law enforcement context;
- The importance of the purpose of the processing must be assessed: This means that, considering the measures taken in the case at hand, the data collection must take into account all relevant factors. These include the nature and gravity of the presumed offence of which the person is accused, the particular circumstances of that offence, any link between that offence and other procedures in progress, and the criminal record or individual profile of the persons in question;
- The principle of data minimisation must be strictly checked. This means, *inter alia*, that only DNA data that does not reveal information about a person's ethnicity or genetic diseases is registered.

According to the ECJ it is up to the referring court to assess the applicable requirements of the LED. However, the judges in Luxembourg emphasised that the case at issue "merely" concerns the police's right to take samples of biometric and genetic data from suspected persons, and not the systematic collection of such data from any accused or suspected person (as decided in its judgment of 26 January 2023 in Case C-205/21 →eucrim 1/2023, 32–33). Furthermore, the economic nature of the offence is not sufficient to exclude the collection of said data from being regarded as strictly necessary.

➤ *The ECJ's reasoning on the lack of a maximum period for data storage*

Regarding the necessity of establishing maximum time limits for storage, the ECJ found that two issues must be distinguished.

First, the need to establish absolute time limits for data storage: In this context, Member States are not required to define absolute time limits, even if sensitive personal data is stored, provided that they foresee periodic reviews of the need to store personal data. If this review concludes that the storage of these data no longer appears to be strictly necessary, the data must be erased.

Second, the need to assess the continuation of storing biometric and genetic data on the basis of internal police rules: The juges in Luxembourg state that that fact is not in itself contrary to Art. 8(2) LED, in so far as those rules require the police to ensure that the condition that the storage of those data is strictly necessary is satisfied and that the discretion of the police is governed by a sufficient framework under national law, including national case-law.

➤ *Put in focus*

With its ruling in the present case, the ECJ goes beyond the opinion of Advocate General *de la Tour* on 27 February 2025. The latter was rather critical of the Czech approach, concluding that the LED requires national legislation to provide for an obligation on the part of the law enforcement authority to assess in each specific case the "strict necessity" of the processing it has performed, or is contemplating performing. He also called for regular reviews of the data retention to be subject to strict procedural safeguards.

However, the ECJ does not apply strict standards to legislation for the collection of biometric and genetic data in criminal proceedings. Laws do not have to regulate the requirements of the LED in detail. The ECJ considers it more important that national law provides clear mechanisms to verify compliance with the LED's requirements, and that national courts are able to monitor the actions of the data controllers. The ECJ also makes it clear that the police must decide on a case-by-case basis whether to collect and record sensitive personal data. Therefore, the case relating to the Czech Police Law differs from cases in which EU Member States permitted the systematic, indiscriminate collection of sensitive data. (TW)

ECJ Clarifies GDPR Information Duties for Body Cameras in Public Transport

On 18 December 2025, the ECJ delivered its judgment in *Integritetsskyddsmyndigheten v AB Storstockholms Lokaltrafik* (Case C-422/24), clarifying which information obligations under the General Data Protection Regulation (GDPR) apply when personal data are collected through body cameras worn by ticket inspectors.

➤ *Background of the case*

The case originated in Sweden and concerned the use of body cameras by ticket inspectors employed by AB Storstockholms Lokaltrafik (SL). The cameras continuously recorded images and sound during inspectors' shifts, using a circular memory system that automatically overwrote footage after a short period unless manually preserved. Inspectors were instructed to retain recordings in situations involving fines or threats.

Following an investigation, the Swedish Data Protection Authority (*Integritetsskyddsmyndigheten*) concluded that SL had infringed Art. 13 GDPR by failing to provide adequate information to data subjects about the processing of their personal data. It imposed an administrative fine of SEK 16 million, of which SEK 4 million related specifically to the information deficit.

While a first-instance court upheld the fine, the Administrative Court of Appeal annulled it, holding that Art. 13 GDPR was not applicable and relying in part on the earlier ECJ's judgment in *Ryneš* (Case C-212/13). The Swedish Supreme Administrative Court then referred the question to the ECJ as to whether Art. 13 GDPR (headed "Information to be provided where personal data are collected from the data sub-

ject" or Art. 14 GDPR (headed "Information to be provided where personal data have not been obtained from the data subject") governs information duties where personal data is collected via body cameras.

➤ *The ECJ's decision and reasoning*

The judges in Luxembourg held that Art. 13 GDPR applied. They emphasised that the decisive criterion for distinguishing between Arts. 13 and 14 GDPR is the source of the data. Art. 13 governs situations in which personal data is collected directly from the data subject, whereas Art. 14 applies only to data obtained from another source.

According to the ECJ, footage captured by body cameras constitutes data collected directly from the data subject, even if the individual plays no active role in providing it. Accepting the application of Art. 14 in such cases would risk allowing the collection of personal data without immediate transparency, potentially enabling hidden surveillance practices. Such an interpretation would be incompatible with the GDPR's objective of ensuring a high level of protection of fundamental rights, in particular Arts. 7 and 8 of the Charter of Fundamental Rights of the EU.

The ECJ noted that its earlier ruling in *Ryneš* did not resolve the distinction between Arts. 13 and 14 GDPR and could not justify excluding Art. 13 in this context. It further clarified that transparency obligations under Art. 13 GDPR could be implemented through a layered approach, for example by combining visible warning signs with more detailed information provided in an easily accessible place.

➤ *What's next?*

The case now returns to the Swedish Supreme Administrative Court, which must resolve the dispute in light of the CJEU's interpretation. More broadly, the judgment provides guidance for public authorities and private operators using body-worn cameras or similar video devices across the EU. Controllers collecting data directly through video recording must ensure that data subjects are informed in accordance with Art. 13 GDPR at the time of collection, subject to the regulation's specific exceptions.

The ruling thus strengthened the transparency requirements applicable to surveillance technologies and clarified the boundaries between Arts. 13 and 14 GDPR in practice. (AP)

ECJ Strengthened Data Protection on Online Marketplaces

On 2 December 2025, the Grand Chamber of the European Court of Justice (ECJ) ruled in Case C-492/23 (*Russmedia Digital and Inform Media Press*) that the operator of an online marketplace is responsible for processing the personal data contained in advertisements published on its platform.

➤ *Background of the case*

The victim of an advertisement with defamatory and offensive content, which had been published by an unknown person on the online marketplace "www.publi24.ro", is demanding non-material damages from the operator, Russmedia Digital (a Romania-based company). According to the advertisement, the person concerned was offering sexual services. The advertisement contained photos and the telephone number of the person concerned. Russmedia Digital removed the material within an hour after the victim's request, as the advertisement was untrue and harmful to her. However, the advertisement was quickly picked up by other websites, where it remained accessible. Russmedia argued that its role is purely technical, merely providing a hosting service. However, it reserves the right to use the content.

The referring Court of Appeal of Cluj, Romania, sought guidance from the ECJ as regards the obligations on the operator of an online market place under the General Data Protection Regulation (GDPR) and as regards the question of whether such an operator may be relieved of those obligations on the basis of the exemption from liability provided for by Art. 14(1) of Directive 2000/31 for intermediary service providers.

➤ *The ECJ's reasoning*

The ECJ justifies its ruling as follows: Although the advertisement is placed by a user, it is only published via the online marketplace on the internet and thus made accessible to internet users. Therefore, before publishing these advertisements, the operator of an online marketplace must take appropriate technical and organisational measures to identify those advertisements that contain sensitive data and verify that the user who is about to place such an advertisement is the person whose sensitive data is contained therein.

If this is not the case, they must verify whether the person whose data is being published has expressly consented to the publication. Without this consent, the operator of an online marketplace must refuse to publish the advertisement in question, unless it falls under one of the other exceptions provided for in the GDPR.

In addition, the operator of an online marketplace must endeavour to prevent advertisements containing sensitive data published on its website from being copied and unlawfully published on other websites. To this end, it must take appropriate technical and organisational security measures.

Lastly, the ECJ clarified that the operator of an online marketplace cannot avoid its obligations under the GDPR by relying on the exemption from liability under the regime of Directive 2000/31. It follows from a combined reading of Art. 1(5)(b) of Directive 2000/31 and Art. 2(4) of the GDPR that the provisions of the Directive, in particular Arts. 12 to 15 thereof, cannot interfere with the regime under the GDPR.

➤ *Put in focus*

Art. 6 of the Digital Services Act (DSA) and Art. 14(1) of Directive 2000/31 (the "e-commerce Directive") include the so-called "provider privilege". Accordingly, where an information society service is provided that consists of the storage of information provided by a recipient of the service, that service provider shall not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. The GDPR does not contain such a clause. As a result, it has been under dispute whether the provider privilege also covered the processing of personal data.

The ECJ has now resolved this conundrum unilaterally in favour of the GDPR. The ruling could have far-reaching consequences for the internet. In any case, it increases the pressure on service providers to carry out preventive checks. (TW)

Victim Protection

Help4U: New Digital Platform Boosts Youth Support Access

Europol and the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC, a specialist research institute based at Sheffield Hallam University, UK) developed a new digital platform called "Help4U" to support children and teenagers experiencing sexual abuse or online harm. This initiative is based on the fact that young victims often turn to online resources first, particularly when they feel overwhelmed or are not ready to speak to someone in person. Initially piloted in five EU Member States, Help4U has expanded to 15 countries since November 2025, with further growth planned from 2026 onwards.

The platform is designed to be private, accessible, and easy to use. It helps young people understand their rights, access trusted information, and connect with appropriate support services. A key feature is its accessibility-driven design, which allows young users to choose how they engage with support – by reading, chatting, or locating nearby services – and using clear, age-appropriate language. The platform also provides for a prominent "quick exit" button allowing users to leave the platform instantly, ensuring their privacy and safety if they feel threatened or uncomfortable. Available in ten different languages, the platform also serves as a resource for parents, educators, and professionals.

Developed through collaboration across law enforcement, psychology, education, data protection, and academia, Help4U represents a coordinated European approach to strengthening protection against online sexual abuse. (CR)

Cooperation

Judicial Cooperation

AG Opinion on Speciality Rule in TCA

On 4 December 2025, Advocate General *Laila Medina* delivered her Opinion in Case C-528/24 ("Boothnesse"). In this case, the ECJ is required to interpret the rule of speciality, a basic safeguard in extradition law, as laid down in Article 625(2) of the TCA (the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part). According to this provision, "a person surrendered may not be prosecuted, sentenced or otherwise deprived of liberty for an offence committed prior to that person's surrender other than that for which the person was surrendered."

➤ *Background of the case and questions referred*

The reference for a preliminary ruling was made by the Irish Supreme Court. Before that court, three defendants objected to their extradition from Ireland to the United Kingdom (UK) on the ground that the arrest warrant issued for the prosecution of fraud did not include their possible prosecution for contempt of court, as the defendants had failed to comply with restraint orders; the UK court had imposed an imprisonment of six months on each defendant for this act. However, according to the UK authorities, "contempt of court" is classified as a civil matter and not as a criminal offence, therefore, the arrest warrant could not include this act.

Essentially, the Irish Supreme Court is seeking guidance from Luxembourg as to whether the term "offence" has an autonomous meaning in EU law and, if so, whether a surrender could be refused on the basis of Art. 625(2) TCA.

➤ *The AG's Opinion*

According to AG *Medina*, the term "offence" in Art. 625(2) TCA requires an autonomous interpretation, independent of the issuing State's formal classification. The decisive factor is whether a conduct or sanction is criminal in nature, as developed by the ECJ's judgment in *Bonda*. In this judgment, the ECJ established a three-step test (in line with the *Engel* criteria developed by the ECtHR): (i) the legal classification under national law; (ii) the intrinsic nature of the offence; and (iii) the severity of the penalty.

If, on the basis of the *Bonda* criteria, the requested judicial authority concludes that the sanction in question is criminal in nature, it must determine

whether a real risk persists that the person concerned would, after surrender, be detained in breach of the rule of speciality. Refusal of surrender can be averted if the issuing State provides adequate guarantees that no such detention will occur. (TW)

European Arrest Warrant

AG Opinion: Refusal of EAW in Case of Disproportionate Sentence

In his Opinion in Case C-583/24 (Tagu) released on 22 January 2026, Advocate General (AG) *Richard de la Tour* addressed the question of whether the threat of enforcement of a manifestly disproportionate custodial sentence can prevent surrender on the basis of a European arrest warrant (EAW).

The reference for a preliminary ruling to the ECJ was prompted by the Rechtbank Amsterdam (District Court of Amsterdam, Netherlands). The court has to decide on the enforcement of an EAW from Romania. The person concerned had been sentenced there to seven years' imprisonment for importing three grams of cannabis and four ecstasy pills, which is the minimum sentence provided for by law. According to the findings of the Amsterdam court, the drugs were intended for personal use and there was no intention to trade.

AG de la Tour emphasises that the mutual recognition of judicial decisions is a fundamental principle of the European arrest warrant and that the determination of the sentence remains, in principle, a matter for the issuing state. Nevertheless, surrender may not take place if the authority has objective, reliable and up-to-date information indicating systemic or generalised deficiencies in the issuing state's compliance with the principle of proportionality of penalties, with the result that the courts have no possibility of individualising the penalty for certain categories of criminal offences. In addition, in the specific individual case, there must be a real risk, based on serious and substantiated grounds, that the person concerned would be exposed to a manifestly and extremely disproportionate penalty after surrender. (TW)

European Investigation Order

ECJ: EIO Can Be Issued Instead of EAW

spot light

In its judgment of 18 December 2025 in Case C-325/24 (*Bissilli*), the European Court of Justice (ECJ) ruled that a European Investigation Order (EIO) can be issued for the temporary transfer or for a videoconference hearing of an accused person held in custody abroad, if the EIO has an evidential objective and is necessary for the purpose of gathering evidence. The judges in Luxembourg also clarified the relationship between the various refusal grounds set out in Directive 2014/41 regarding the European Investigation Order in criminal matters (EIO Directive).

➤ *Background to the case and questions referred*

In the case at issue, the Tribunale ordinario di Firenze (District Court of Florence, Italy) is conducting criminal proceedings against HG on charges of participation in a criminal organisation and drug trafficking. The proceedings were conducted in absence of HG but he was represented by a lawyer. HG's lawyer requested that he be heard at the trial, as he is serving a custodial sentence in Belgium. Consequently, the Florence court issued an EIO for the purpose of hearing HG by videoconference. However, the Belgian authorities refused to execute the EIO, arguing that Belgian law does not allow for the videoconferencing of accused persons during their trial, and that the appearance of an accused person at his/her trial by videoconference is contrary to the right to a fair trial (and thus contrary to the fundamental principles of Belgian law). Belgian authorities also declined HG's temporary transfer to Italy.

In essence, the Florence District Court sought guidance from the ECJ as to whether it is entitled to issue EIOs for the accused person's hearing by videoconference or his temporary transfer, given that these measures would not only ensure HG's appearance at trial but also have an evidential purpose. In addition, the Florence District Court asked whether the Belgian authorities could justify refusing to execute such EIOs without examining the concrete circumstance of the case and the safeguards enshrined in Italian law.

➤ *The ECJ's reasoning: EIO or EAW?*

First, the ECJ considered whether the Italian judicial authorities are entitled to issue an EIO if the measures in question – hearing an accused person by videoconference or temporarily transferring that person (Arts. 3, 22, and 24 of the EIO Directive) – have the purpose of both to obtain evidence and to enable the accused person's appearance at his/her trial. Or would such an EIO circumvent the surrender rules on the basis of the European Arrest Warrant (EAW)?

The ECJ concluded that, based on the wording of the relevant provisions in the EIO Directive, their context and the Directive's objectives, the authorities of EU Member States are not precluded from issuing an EIO if the investigative measure has a purpose of gathering evidence and incidentally ensures the presence of the accused at their trial. However, the ECJ makes an important clarification: it can be deduced from both Art. 22 and Art. 24 of the EIO Directive that an EIO may only serve as the basis for the accused's participation in the main hearing for as long as is necessary to obtain evidence.

➤ *Refusal to hear an accused person by videoconference?*

Regarding the various grounds giving the possibility for the executing au-

thorities to refuse an EIO concerning the organisation of a hearing by videoconference of the accused person during the criminal trial, the ECJ clarified the following points:

- Art. 24(2) of the EIO Directive provides for specific grounds for the non-recognition of a videoconference concerning suspected or accused persons. This ground would have no real utility if a refusal could also be based on Art. 10(5) of the EIO Directive, which allows for refusal if the requested measure does not exist or is not available in a similar domestic case in the executing Member State.
- However, Art. 24(2) of the EIO Directive does not deprive the executing authority from applying the refusal grounds established in Art. 11(1), in particular Art. 11(1)(h).
- The refusal ground in Art. 24(2)(b), which states that the execution of a videoconference concerning a suspected or accused person would be contrary to the fundamental principles of the law of the executing State, is independent from the refusal ground in Art. 11(1))(f), which relates to a videoconference that would run counter fundamental rights.

Lastly, the ECJ ruled that the executing State may adopt general guidelines for applying the refusal ground in Art. 24(2)(b) – refusal due to fundamental principles of the law of the executing State – provided that the executing authorities carry out an individual examination considering all the relevant circumstances of the case.

➤ *Put in focus*

As far as can be seen, the ruling in *Bissilli* is the ECJ's first judgment that tackles the question of whether a European Investigation Order can be issued instead of a European Arrest Warrant. This is important as discussions have gained momentum favouring the increased possibilities to hear defendants who are staying abroad via videoconference in the course of their criminal proceedings, including the trial. It remains to be seen whether the delimitation focusing on the purpose of the measure can be implemented in practice without major distortions.

In the specific case at hand, the ECJ paved the way for the Italian court to issue an EIO allowing the court to hear the defendant either via videoconference or via his temporary transfer. The judges in Luxembourg also made clear that the executing authorities cannot base their decision of refusal on general justifications or general guidelines, including those derived from the case law of supreme or constitutional courts. However, the ECJ's ruling does not answer all questions. For instance, it remains unclear when the "purpose of gathering evidence" as the essential element of an EIO is achieved and when a hearing shifts "to a transfer for the purposes of prosecution", as stated in para. 59 of the judgement.

Furthermore, the ECJ avoided making a clear statement on whether the Belgian judicial authorities can in effect refuse the execution of the EIO in question again. For example, the ECJ did not respond to the referring court's argument that a refusal is not possible due to fair trial considerations, given that Italian law provides sufficient procedural safeguards for hearings by videoconference for accused persons. The yardstick for verifying concerns relating to fundamental rights concerns remained unanswered.

In the specific case, the issues might be resolved as it was the defendant's lawyer who requested the hearing. Therefore, it would be contrary to his own interests if the EIO were refused again in the country "of his current residence". (TW)

Law Enforcement Cooperation

JHA Council Discusses Internal Security Implications of Drones

At the Council meeting on 8 December 2025, the Home Affairs Ministers of EU Member States discussed common law enforcement measures to address the malicious use of drones. Possible EU actions could include better coordination of anti-drone activities, harmonisation of anti-drone systems standards, and increased funding in research and innovation.

In preparation of the meeting, the Danish Council Presidency circulated a paper outlining the internal security implications of drones, following several recent incidents involving "Unmanned Aircraft Systems" (UAS) that threatened public spaces and critical infrastructure across Europe. The paper also provided an overview of the instruments in place at the EU level, such as the Counter-drone Expert Group (C-UASG), the establishment of a "Counter-Drone Centre of Excellence" within the Joint Research Centre, and the planned extension of the counter-drone training for law enforcement to other security authorities and private sector stakeholders. The Danish Council Presidency referred to plans for the new Multiannual Financial Framework to provide additional funding for "the development and deployment of European civilian, dual-use and defence drone and counter-drone solutions". It also highlighted projects led by Frontex and Europol, harnessing the potential of UAS technologies for law enforcement and border management, and to mitigate the security risks posed by their illicit use. The debate followed an earlier exchange at the Justice and Home Affairs Council in October 2025 and the European Council's call for strengthened joint efforts to enhance counterdrone and air-defence capabilities.

For the December meeting, delegations were invited to focus on the law enforcement dimension of the issue and to identify both the main operational challenges and possible further EU-level action in this rapidly evolving field. (TW)

Council of Europe

Reported by Thomas Wahl (TW) and Dr. Anna Pingen (AP)

Foundations

Human Rights Issues

Russia Withdraws from Anti-Torture Convention

On 30 October 2025, Russia officially informed the Council of Europe that the country was denouncing the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (ECPT). The denunciation will become effective on 1 November 2026 as under Art. 22, paragraph 2, of the ECPT, the Russian Federation remains bound by the ECPT for one year after the date of receipt of the notification by the Secretary General.

Russia joined the ECPT in 1998 but has frequently not cooperated with the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT), which implements the countries' obligation under the ECPT.

Russia had already been excluded from the Council of Europe in 2022, but remained formally bound by the ECPT. Its withdrawal therefore marks the loss of one of the last remaining European monitoring mechanisms applicable to places of detention in Russia. The withdrawal from the Council of Europe's Anti-Torture Convention means above all that Russia no longer accepts any independent external oversight of places of deprivation of liberty. (TW)

Areas of Crime

Corruption

New GRECO Paper: Whistleblower Protection in Law Enforcement

spot light

On 10 December 2025, GRECO published a new thematic paper that outlines GRECO's findings on and approach to whistleblower protection within the context of its Fifth Evaluation Round. The Fifth Evaluation Round focused on the prevention of corruption and the promotion of integrity within central governments (persons with top executive functions) and law enforcement agencies.

GRECO highlights that the significant role of whistleblowers in the fight against corruption, in both the public and the private sector, and notes that the Council of Europe has pioneered high standards of whistleblower protection. In the 5th evaluation round, GRECO dedicated a specific chapter to whistleblower protection in the police aiming at breaking the culture of "codes of silence" and promoting integrity within law enforcement agencies. The thematic paper presents a review of GRECO's findings in three areas:

- The legal framework for whistleblower protection;
- The provision of training, information and advice;
- The monitoring of whistleblower protection.

Another chapter spotlights examples of good or promising practices from member states that could inform future reforms.

Overall, GRECO found that important gaps remain although progress in whistleblower protection has been made in many member states. According to GRECO, the 5th round of evaluation called to mind that member states should address the following issues:

- Adequate rules on whistleblower protection;
- Clearer reporting channels;
- Strong safeguards against both direct and subtle forms of retaliation;
- Ensure strict confidentiality.

Several member states have been required by GRECO to review their legislation on whistleblower protection, with a view to strengthening its effectiveness. Many other countries were asked to prohibit reprisals within police services. Moreover, GRECO stressed the need to raise awareness, provide specialised training, and collect and monitor data to allow assessment of effectiveness.

Lastly, GRECO emphasised that it will continue to explore several issues relating to whistleblowing in the 6th Evaluation Round, which focuses on preventing corruption and promoting integrity at the sub-national level and launched in 2025. (TW)

GRECO Urges Poland to Make Progress in Anti-Corruption Reform

Following a meeting with senior officials of the Polish government and parliament on 28 November 2025, a GRECO delegation urged the Polish authorities to implement the open recommendations made during the fourth and fifth evaluation rounds as they are essential for ensuring full alignment with the Council of Europe's anti-corruption standards. GRECO's delegation, headed by its President *David Meyer,* noted that reform had stalled during the national-conservative PiS government, but that it is important to

achieve tangible results in anti-corruption reform.

During the 4th evaluation round, GRECO expressed serveral concerns over the 2017 judicial reform entailing increased influence of the legislative and executive branches over the judiciary (→eucrim 1/2013, 13). During the 5th evaluation round, GRECO found fault with the limited progress in strengthening the integrity framework for people in senior executive roles in government, as well as with anti-corruption efforts within law enforcement authorities (→eucrim 1/2019, 44). According to GRECO, more rapid action is needed to restore judicial independence and reinforce government integrity.

GRECO will further assess the measures taken by the Polish authorities under the 4th and 5th evaluation rounds in 2026 and 2027, respectively. (TW)

GRECO: Ad hoc Report on Slovakia

At the end of August 2025, GRECO published an *ad hoc* report on recent changes to criminal law and institutional reforms in the Slovak Republic launched in 2024. The report – based on Rule 34 of GRECO's Rules of Procedure (→eucrim 1/2020, 32) – assessed the extent to which the reforms comply with European standards. GRECO expressed concerns over the measures taken, including the application of the fast-track legislative procedure, the shortening of limitation periods, reduced criminal penalties for corruption offences and interventions in police and prosecutorial organisation. The report addresses several recommendations to the Slovak government, including:

- Conducting a comprehensive review of the rules governing the use of the fast-track legislative procedure and considering revision of this procedure in order to restrict its application to strictly exceptional cases, which are clearly defined and duly justified;
- Enabling public consultation to draft legislation and ensuring a meaningful opportunity for stakeholder participation to provide input prior to the adoption of legislation;
- Revising legislation to provide for a sufficiently long limitation period and sentencing framework for all corruption offences;
- Conducting a comprehensive review of the current framework for prosecutorial specialisation in corruption cases;
- Developing a formal plan for specialisation and continued professional development of prosecutors, in order to ensure compliance with anti-corruption standards;
- Developing, publishing and implementing a plan for the specialisation of investigating police officers, involving specific job descriptions and specific, measurable, achievable, realistic and time-specific targets;
- Repealing Article 326a of the Slovak Criminal Code which provides for the offence of "bending the law", as its vague wording impacts the judges' ability to take decisions freely and independently, based exclusively on the relevant laws; this provision ultimately leads to self-censorship and undermines judicial independence.

GRECO invites the Slovak authorities to report back on measures taken against the concerning issues by 31 December 2026. (TW)

GRECO's Recent Compliance Reports

In the recent months, GRECO published a series of compliance, follow-up and progress reports regarding the implementation of GRECO recommendations made vis-à-vis member states during the fourth and fifth evaluation rounds. The 4th evaluation round focused on preventing corruption in respect of members of parliament, judges, and prosecutors. The 5th round focused on the prevention of corruption and the promotion of integrity within central governments (persons with top executive functions) and law enforcement agencies (for the single country reports →previous eucrim issues). The different steps of GRECO's evaluation and compliance procedure, including its termination, are regulated in GRECO's Rules of Procedure. The Rules of Procedure were adopted in 1999 and lastly amended in 2017 taking account of the 5th evaluation round.

GRECO is currently in transition between the fourth/fifth and sixth evaluation round. The 6th evaluation round was launched in 2025 focusing on preventing corruption and promoting integrity at the sub-national level. The following provides an overview of the published compliance reports on the respective GRECO member states since July 2025 in chronological order. They can concern both the 4th and 5th evaluation round. Website links are provided to the full text of the report and the corresponding press release of GRECO as well as the cross-reference to the news on the respective evaluation report in *eucrim*.

- 4 July 2025: **The Netherlands** – Follow-up Report, concluding that the country is not yet in sufficient compliance with the recommendations made in the 5th round evaluation report. Tangible and robust measures are needed for instance with regard to the adoption of a dedicated integrity policy and a reporting mechanisms for gifts and financial interests in the police. The Dutch authorities are requested to provide a progress report with regard to the implementation of the outstanding recommendations by 31 March 2026.
- 9 July 2025: **North Macedonia** – Follow-up Report, in which GRECO positively notes progress in the implementation of the open recommendations of the 5th evaluation round. In particular, GRECO welcomes the steps taken to improve transparency and promote integrity as regards persons entrusted with top executive functions and the legislative reform

aimed at strengthening the operational independence of the police and its internal and external oversight mechanisms. GRECO closes its compliance procedure for North Macedonia under this round.

■ 30 July 2025: **Portugal** – *Interim* Compliance Report, finding that the majority of the recommendations contained in the 2015 4th round evaluation report remain only partially implemented. GRECO notes, *inter alia*, that lobbying remains unregulated and the composition of judicial councils to safeguard judicial independence has not been enhanced. As the level of compliance is found "globally unsatisfactory", the Portuguese authorities are requested to provide a progress report on the implementation of the outstanding recommendations by 31 March 2026.

■ 1 August 2025: **Spain** – Follow-up Report, finding that the Spanish authorities should intensify their efforts to implement planned reforms to strengthen anti-corruption mechanisms regarding top executive functions of the central government and law enforcement agencies (National Police and Guardia Civil). GRECO concludes that Spain is not in sufficient compliance with the recommendations made in the 5th evaluation round. GRECO requests the Spanish authorities to provide a progress report by 30 June 2026.

■ 5 August 2025: **Romania** – Compliance Report, welcoming key improvement in the prevention of corruption at top executive functions and the Romanian Police and Gendarmerie. However, further progress is needed within the next 18 months to achieve an adequate level of compliance with a number of recommendations set out in the 5th evaluation round report, such as effective integrity checks for top executive functions and the establishment of a dedicated oversight mechanism of the access-to-information legislation. Romania should submit additional information on the implementation of these recommendations by 31 December 2026.

■ 7 August 2025: **Poland** – Follow-up Report, assessing that some progress has been made in anti-corruption measures in central governments, but progress is required in other areas, including the Polish Police and Boarder Guard; given that Poland only implemented 3 out of 21 recommendations set out in the 5th round evaluation report in a satisfactory manner, GRECO requests Poland to provide a progress report by 31 March 2026.

■ 8 August 2025: **Germany** – Compliance Report, concluding that the country needs to make further progress in implementating of a number of recommendations made in the 2020 5th round evaluation report, such as raising integrity standards for persons at top executive functions, improving public access to information at federal level, strengthening the screening processes of new recruits in the Federal Police, and ensuring stricter and more proactive internal oversight within the Federal Police. Germany is asked to provide a progress report on the outstanding recommendations by 31 March 2026.

■ 18 August 2025: **Denmark** – Follow-up Report, voicing GRECO's dissatisfaction with the lack of progress made by the country (see also →eucrim 1/2025, 39): Denmark has dealt in a satisfactory manner with only two of the fourteen recommendations contained in the 2019 5th round evaluation report; of the other recommendations, one remains partly implemented and eleven remain not implemented. Several anti-corruption measures are still needed with regard to persons with top executive functions and the Danish police. GRECO urges Denmark to report on tangible progress by 30 June 2026.

■ 2 September 2025: **Portugal** – Compliance Report, concluding that the country has yet to implement 10 out of 28 recommendations issued in the 2023 5th round evaluation report, while 18 recommendation have been partially implemented so far. GRECO acknowledges key progress made in anti-corruption measures regarding persons with top executive functions of the central government and the Portuguese law enforcement forces (the Public Security Police (PSP) and the National Republican Guard (GNR)). However, many determined actions are still needed, such as strengthened integrity controls and dedicated anti-corruption strategies for the PSP/GNR. Portuguese authorities should report on the progress achieved in implementing GRECO's recommendations by 30 September 2026.

■ 4 September 2025: **Slovak Republic** – Follow-up Report, concluding that most of GRECO's recommendations in the 2019 5th round evaluation report have remained unimplemented. Even though Slovakia launched some anti-corruption measures, such as a code of ethics for police forces, no visible progress has been made in many other matters, such as integrity and whistleblower protection within the police. As the Slovak Republic is not in sufficient compliance with the recommendations, GRECO requires a progress report by 30 June 2026.

■ 16 September 2025: **Cyprus** – Compliance Report, noting that Cyprus has made significant progress in enhancing its legal framework to prevent corruption and promote integrity in the central government and the police. However, further reforms are still needed to comply with GRECO's recommendations in the 5th round evaluation report, such as consolidating integrity standards, and streamlining oversight and accountability mechanisms for the police. Cypriot authorities are invited to submit additional information on the implementation of outstanding recommendations by 31 December 2026.

■ 27 November 2025: **United Kingdom** – Follow-up Report, acknowledging considerable progress in implementing GRECO's recommendations in the 5th evaluation round. GRECO highlights that the United Kingdom undertook several measures to promote transparency and integrity of persons with top executive functions in government. Looking at law enforcement agencies, GRECO welcomes the commendable progress made in implementing all of its recommendations satisfactorily. GRECO terminates the Fifth Round compliance procedure with respect to the United Kingdom.

■ 28 November 2025: **Malta** – Follow-up Report, acknowledging some advances in Malta's criminal justice system and within the Police Force, but stressing that important shortcomings persist, and progress remains limited in in the vast majority of areas fundamental to promoting integrity and preventing corruption in the executive as set out in GRECO's 5th round evaluation report. This includes the failures to adopt an integrity strategy for persons in top executive functions and to resolve obstacles in access to information. As regards law enforcement authorities, more notable progress has been achieved, but further developments are required, e.g. with regard to a risk-assessment based anti-corruption strategy, sufficient operational independence and political neutrality of the Police Force. GRECO calls on Malta to take determined steps to advance reforms in the areas identified and report on progress in implementing the outstanding recommendations by 30 June 2026.

■ 4 December 2025: **Liechtenstein** – Compliance Report, concluding that 6 out of 16 recommendations from the 2020 4th round evaluation report are yet to be implemented. GRECO regrets that only limited progress has been achieved with regard to members of parliament, such as the recommendation to make the legislative process at the level of parliamentary commissions more transparent. As regards judges, additional steps must be taken to increase the role of the judiciary in the selection process of judges, while all recommendations have bee implemented with regard to prosecutors. GRECO asks Liechtenstein to submit additional information on the measures taken to implement the outstanding recommendations by 30 June 2026.

■ 5 December 2025: **Ireland** – Follow-up Report, closing GRECO's evaluation of Ireland´s legal and institutional framework to prevent corruption in respect of the recommendations set out in the 4th evaluation round. Even though three out of 11 recommendations haven been partially implemented only, GRECO acknowledges Ireland's legislative reforms to improve ethical conduct of members of parliament and enhanced financial disclosure requirements. Also appointments and nominations to judicial office improved and are more transparent.

■ 11 December 2025: **France** – Follow-up Report, finding that only 4 of 18 recommendations set out in the 5th round evaluation report have satisfactorily been implemented. With regard to top executive functions, GRECO notes some progress, particularly in raising awareness of integrity issues, but the country's strategic framework for tackling corruption could be strengthened. In the area of law enforcement, GRECO acknowledges the increased attention to corruption risks within the National Police and the National Gendarmerie, but certain recommendations have remained untouched. French authorities should provide a progress report by 30 November 2026.

■ 17 December 2025: **Iceland** – Follow-up Report, welcoming a number of positive efforts to address GRECO's recommendations in the 5th round evaluation report. Iceland aligned with most recommendations with regard to both persons in top executive functions in government and law enforcement authorities. GRECO terminates the 5th round compliance procedure with respect to Iceland.

■ 6 January 2025: **Belgium** – two Follow-up Reports, assessing the country's efforts to implement recommendations in the 4th and 5th evaluation round. The follow-up report on the 4th evaluation round (prevention of corruption and promotion of integrity among members of parliament, judges and prosecutors) concludes that Belgium has made slight progress in implementing the recommendations; the main issues in GRECO's 2014 evaluation report have remained unresolved. Nonetheless, GRECO terminates the fourth round compliance procedure in respect of Belgium. The follow-up report on the 2020 5th evaluation round, concludes that Belgium still needs to make efforts in both areas under scrutiny, i.e. the prevention of corruption with regard to persons in top executive functions and the Federal Police. Many recommendations in the 5th round evaluation report are yet to be addressed or fully implemented. Accordingly, Belgium is required to report back on progress made in these areas by 30 November 2026.

■ 12 January 2025: **Croatia** – Follow-up Report, underlying that the country should take above all more determined action to implement several outstanding recommendations set out in the 5th evaluation round report with regard to the prevention corruption among top executive functions of the central government. Overall, GRECO is satisfied with the progress made in the area of law enforcement, where measures to strengthen police integrity and to prevent police corruption were adopted. Croatia is invited to report back on progress by 30 November 2026.

■ 22 January 2025: **Romania** – Follow-up Report, calling on Romania to further implement recommendations from the 4th evaluation round in view of corruption prevention among members of parliament. Also progress on the regulation of lobbying has been made, no progress has been reported on other outstanding recommendations, such as the prevention of conflicts of interests and transparency of parliamentary work. As Romania has still not implement five outstanding recommendations, GRECO asks the country to report back on implementation efforts by 30 November 2026.

■ 12 Feburary 2025: **Finland** – Follow-up Report, concluding that the 5th round compliance procedure in respect of Finland can be closed. GRECO recognises the country's progress made in implementing anti-corruption reforms concerning top executive functions in central government and law enforcement agencies. *Inter alia*, GRECO highlights the enforcement and sanction mechanisms in place against civil servants and the provision of integrity training. With respect to law enforcement agencies, GRECO concludes that all recommendations of the 5th round evaluation report have been fully implemented. (TW)

Money Laundering

MONEYVAL: Decisions Adopted at Plenary Meeting

From 15 to 18 December 2025, the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) held its plenary meeting in Strasbourg. The meeting convened around 200 AML/CFT experts from approximately 50 jurisdictions and international organisations.

It was chaired by *Nicola Muccioli* (San Marino) who was re-elected as the Committee's chair for a second mandate.

As important outcomes, the plenary adopted the 6th round mutual evaluation report on Serbia, the second country that was evaluated under the current evaluation cycle. With regard to the 5th evaluation round, the plenary adopted follow-up reports for Azerbaijan, Croatia, Estonia, Georgia, Montenegro, Poland and Slovakia. Czechia and Slovakia were removed from the Compliance Enhancing Procedures (CEPs) process, whereas it was proposed that Georgia remain in Step 1 of the CEP and that Poland also be placed in Step 1 of the CEPs.

The plenary also approved two typologies' reports targeting ML/TF risks:

■ Risks posed by virtual assets;

■ Risks arising from armed conflicts. (TW)

Environmental Crime

CoE Opens New Convention on Environmental Crime for Signature

spot light

On 3 December 2025, the Council of Europe opened the Convention on the Protection of the Environment through Criminal Law (CETS No. 228) for signature, marking a significant step in the development of international legal tools to address environmental crime. The new convention seeks to strengthen criminal justice responses to serious environmental harm and promote closer cooperation between states in the investigation and prosecution of such offences.

At the opening ceremony in Strasbourg, the European Union and two Council of Europe member states (Moldova and Portugal) became the first signatories. Council of Europe Secretary General *Alain Berset* called on other states to join the treaty swiftly, stressing that stronger collective action was necessary to address environmental crimes that threaten ecosystems, human health, and economic stability.

The convention forms part of broader Council of Europe initiatives addressing environmental protection and responds to the growing recognition that environmental degradation is linked to the global challenges of climate change, biodiversity loss, and pollution. The instrument focuses specifically on the role of criminal law in tackling environmental damage and aims to close enforcement gaps that have historically allowed serious environmental offences to remain insufficiently investigated or prosecuted.

In substance, the Convention obliges State Parties to do the following:

■ Criminalising a range of serious acts causing environmental harm with regard to: pollution, products and substances; waste; installations; ships; natural resources; and biodiversity;

■ Introducing provisions that address intentional conduct leading to environmental disasters, comparable in scale to what has been described in international debate as "ecocide";

■ Addressing corporate liability, the liability of legal persons, and sanctions that must be effective, proportionate, and dissuasive.

State Parties are also obliged to establish integrated policies to prevent and combat the commission of any offence established in the Convention, including the establishment and publication of a respective national strategy. Parties shall also allocate appropriate financial and human resources to prevent and combat the commission of the determined environmental offences. With regard to prevention, Parties need to promote or organise information and awareness-raising campaigns relating to preventing and combating environmental crime. Interestingly, the Convention also provides that Parties can stipulate to grant persons who have sufficient interest or allege a vi-

olation of a right, as well as non-governmental organisations promoting environmental protection, the right to participate in criminal proceedings concerning offences established in accordance with this Convention.

Last but not least, the treaty promotes international cooperation in investigations and prosecutions and provides for a monitoring mechanism to oversee implementation by participating states.

Entry into force will occur once the convention has been ratified by at least ten parties, including a minimum of eight Council of Europe member states. It will also be open to accession by non-Council of Europe member states once it becomes operative – reflecting the transnational nature of environmental crime.

By establishing common criminal law standards and encouraging stronger cross-border cooperation, the new convention is expected to enhance accountability for environmental harm and reinforce the role of criminal justice systems in environmental protection. *Eucrim's* documentation database on the Council of Europe conventions will provide updates on signatures, ratifications and accessions of/to the new Convention. (AP/TW)

Legislation

Council of Europe Conventions – Update

The following table shows the developments in connection with ratifications and accessions of tax/criminal/security law-related Council of Europe Conventions. It follows up the list in eucrim 1/2024, p. 52 and records selected developments from 1 January 2025 to mid-May 2026. The table is regularly updated (including *signatures* to the CoE Conventions) on the eucrim website at <https://eucrim.eu/documentation/ratifications/>. (TW)

Council of Europe Treaty	State	Date of ratification (r); accession (a)
Convention establishing an International Claims Commission for Ukraine (ETS No. 229)	Latvia	20 May 2026 (r)
	Ukraine	15 May 2026 (r)
	European Union	15 May 2026 (r)
	Ireland	15 May 2026 (r)
	Estonia	30 April 2026 (r)
	Iceland	28 April 2026 (r)
Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (ETS No. 225)	European Union	20 May 2026 (r)
Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (ETS No. 224)	Costa Rica	15 April 2026 (r)
	Hungary	5 February 2026 (r)
Protocol amending the Additional Protocol to the Convention on the Transfer of Sentenced Persons (ETS No. 222)	Cyprus	14 November 2025 (r)
	Sweden	6 November 2025 (r)
Council of Europe Convention on Offences relating to Cultural Property (ETS No. 221)	Albania	14 February 2025 (r)
Council of Europe Convention on an Integrated Safety, Security and Service Approach at Football Matches and Other Sports Events (ETS No. 218)	Cyprus	14. November 2025 (r)
	Hungary	8 July 2025 (r)
	Serbia	23 January 2025 (r)
Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (ETS No. 217)	Liechtenstein	15 May 2026 (r)
Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (ETS No. 215)	Armenia	15. May 2026 (r)
	San Marino	4 June 2025 (r)
	Serbia	23. January 2025 (r)
Protocol No. 16 to the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 214)	Latvia	25 November 2025 (r)
	Spain	31 July 2025 (r)
Fourth Additional Protocol to the European Convention on Extradition (ETS No. 212)	Montenegro	14 January 2026 (r)
	Cyprus	14 November 2025 (r)
Third Additional Protocol to the European Convention on Extradition (ETS No. 209)	Montenegro	14 January 2026 (r)
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)	Malta	4 June 2025 (r)
	Rwanda	10 January 2025 (a)
Convention on Cybercrime (ETS No. 185)	Papua New Guinea	6 May 2026 (a)
	New Zealand	28 August 2025 (a)
	Sao Tome and Principe	5 June 2025 (a)
	Vanuatu	5 June 2025 (a)
	Rwanda	10 January 2025 (a)
Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182)	Iceland	14 April 2026 (r)
Convention on Mutual Administrative Assistance in Tax Matters (ETS No. 127)	Fiji	26 January 2026 (r)
	Madagascar	28 July 2025 (r)
	Philippines	7 January 2025 (r)
	Trinidad and Tobago	3 December 2024 (r)

Articles

Fil Rouge

Surveillance lies at the heart of this *eucrim* issue. Together, the contributions explore this topic from several perspectives, ranging from the empirical measurement of surveillance practices to the legal challenges arising from large-scale, cross-border investigations. However, they all address the same fundamental question: How can surveillance practices, and the evidence derived from them, be controlled within an increasingly transnational environment that is beyond the scope of any single legal system?

The article section opens with a contribution by *Maxime Lassalle-Han* and *Salomé Lannier* on the EncroChat operation. The authors trace the development of one of the most significant law enforcement operations in recent European criminal law history, connecting French national proceedings with subsequent litigation before the Court of Justice of the European Union and the European Court of Human Rights. The case exemplifies the emergence of data-driven investigations, in which large-scale data collection, cross-border transmission, and reuse in domestic (criminal) proceedings become crucial components of law enforcement. At the same time, the case reveals significant tensions within existing legal frameworks, particularly with regard to transparency, procedural safeguards, and the ability of defendants to challenge the collection and transfer of data.

These tensions are taken up and critically examined by *Thomas Wahl* in his analysis of recent German court decisions on the ANOM operation. Both the Federal Court of Justice and the Federal Constitutional Court accepted the use of evidence obtained through a highly opaque transnational operation conducted by the U.S. Federal Bureau of Investigations (FBI), relying on principles such as mutual trust and the *lex fori* approach. Wahl argues that this extension of established doctrines to qualitatively different forms of cooperation risks narrow the scope of judicial review and weaken the protective function of the *ordre public* exception. In particular, where the chain of evidence is shaped by foreign authorities and remains largely inaccessible, traditional mechanisms of procedural control reach their limits.

The contribution by *Michael Kilchling* and *Sabrina Ellebrecht* broadens the perspective by addressing a fundamental blind spot in current debates. Discussions about surveillance powers – whether focused on their expansion, limitation, or reform – often take place without a reliable empirical understanding of how these powers are actually used in practice. The authors present the findings of the MPI-CSL's Surveillance Barometer (Überwachungsbarometer), a completed research project that combines normative assessment with quantitative data to systematically capture, for the first time, the cumulative impact of surveillance measures in Germany. By doing so, they shift the focus from abstract legality to the concrete impact of surveillance on the extent of fundamental rights protection – and establish an empirical baseline for assessing future legislative changes. Ultimately, they discuss how the findings from the German study could inform the development of a Europe-wide transparency monitoring system.

The final contributions by *Lukasz Zygmunt* and by *Ralf Riegel and Teresa Steiger* move beyond the immediate context of surveillance and address the broader legal architecture of international cooperation (building on the last two eucrim issues, which focused on the current challenges of judicial cooperation and the external dimension of justice and home affairs). *Zygmunt* examines a newly concluded mutual legal assistance treaty between Poland and Indonesia. According to the author, the treaty also includes modern forms of assistance, such as the possibility of conducting hearings by videoconference. *Riegel* and *Steiger* present the evolving framework of cooperation between Germany and Taiwan; the two countries concluded a declaration for the facilitation of mutual legal assistance. Both contributions illuminate the structural conditions under which transnational criminal enforcement operates, including the formalisation of cooperation mechanisms and the search for legal solutions in politically and legally complex settings.

Dr. Anna Pingen,
Co-Editor at eucrim & Postdoc Researcher at the Chair for German, European, and International Criminal Law (Prof. Zimmermann), University of Freiburg

EncroChat – A Judicial Chronology

Interpretations from Paris, Strasbourg and Luxembourg Courts

Maxime Lassalle-Han and Salomé Lannier

The EncroChat investigation marks a turning point in European criminal justice, revealing unprecedented legal and technical challenges that arose from the hacking of encrypted communication devices ("cryptophones"). The operation originated in France and escalated with the deployment of Trojan-style malware, which enabled the collection of data from over 66,000 cryptophone users worldwide. This article provides a detailed timeline of the case, tracing its development from national proceedings to significant rulings by the European Court of Justice and the European Court of Human Rights. It examines the former's interpretation of the Directive on the European Investigation Order and the latter's rejection of challenges arising from the European Convention on Human Rights. By bridging French and European case law and literature, this article fills a gap in existing literature and contributes to ongoing discussions on digital surveillance, privacy, and procedural safeguards in transnational criminal investigations.

I. Introduction

Emerging as landmarks in the evolution of investigative techniques, the EncroChat case, and shortly thereafter, the SkyECC case, signalled the onset of a data-centric era in criminal justice. These cases undoubtedly embody a profound transformation in investigative methods. *Oerlemans* and *Royer* refer to this phenomenon as the rise of data-driven investigations, which they define as "the processing of data that has been collected by law enforcement authorities in an earlier phase, which is then enriched and linked with other data for future investigations."[1]

The EncroChat case was the first major investigation to involve the use of cryptophones, or encrypted messaging services, which are designed to guarantee the anonymity of communications often allegedly led by criminals.[2] The case has become emblematic of both the technical limits of such systems and the legal challenges arising from the investigative techniques employed to bypass encryption.

The case's scale prompted courts in various jurisdictions to review the circumstances under which data were collected in France, and how these data were transferred and subsequently used in criminal proceedings throughout Europe. Three key dimensions can be distinguished:

- The collection of data in France, in the context of an investigation targeting the EncroChat system, considering that the systems itself was deemed illegal, and conducted without any individualised suspicion against its users;
- The cooperation among countries, notably the sharing of data through European instruments of mutual legal assistance in criminal matters;
- The use of these data in domestic proceedings, both in France and abroad.

Each of these dimensions raises novel and fundamental questions, prompting referrals to both the European Court of Justice (ECJ) in Luxembourg and the European Court of Human Rights (ECtHR) in Strasbourg. In France, the Constitutional Council (*Conseil constitutionnel*) and the Court of cassation (*Cour de cassation*)[3] were also called upon to rule on various aspects of the case.

Language barriers may have kept scholars from providing a comprehensive account of the origins, legal framework, and subsequent case law relating to the EncroChat case in France. So far, most analyses have focused on the broader fundamental rights implications before European supranational courts. Yet, the peculiarities of French criminal procedure and the early judicial decisions adopted at the national level have directly impacted subsequent European proceedings. Against this backdrop, this article seeks to address this gap by connecting French and European case law, and by consolidating critical perspectives on relevant judicial outcomes. It provides a review of the case from the initial investigation to the most recent domestic and European decisions delivered in 2025 concerning the French operation itself.

II. The EncroChat Investigation

The EncroChat chronology is difficult to piece together, as dates, translations and explanations have been scattered among European reports as well as national and European court decisions. According to the documents referred to here,[4] the EncroChat investigation can be retraced as outlined in the following timeline chart (see pages below). It distinguishes between the events that happened in France and events that involved European cooperation.

Timeline of the EncroChat Investigation

Operation in France

2017

Law enforcement authorities in France identify EncroChat as a provider of encrypted mobile devices that were increasingly being used by individuals involved in organised criminal activities.

2018

15 November 2018
The *Gendarmerie* — a branch of law enforcement operating under military status but vested with judicial police powers in specific contexts – opens a preliminary investigation (*enquête préliminaire*) after further scrutiny of the initial discovery.

7 December 2018
The public prosecutor's office of the Specialised Inter-Regional Jurisdiction (*Juridiction InterRégionale Spécialisée* – JIRS) in Lille formally confirms the investigation. The case is pursued under several criminal charges, including conspiracy to commit crimes or offences, and violations of legislation governing cryptographic technologies.

December 2018
Investigators locate a server linked to EncroChat in Roubaix, northern France. Subsequently, the Investigating Chamber (*Chambre de l'instruction*) of the Lille Court of Appeal authorises a data capture measure (*captation de données*) under Article 706-102-1 of the French Code of Criminal Procedure. The operation focuses exclusively on the server infrastructure and not yet extends to the encrypted mobile devices themselves.

21 December 2018
The liberty and custody judge (*juge des libertés et de la detention)** authorises the seizure and copy of data stored on the server.** Access is limited to encrypted content and metadata, without decryption or direct access to communications.

2019

October 2019
A second authorisation is granted by the liberty and custody judge, allowing investigators to continue copying server data (access remains limited to encrypted content and metadata)

2020

30 January 2020
The liberty and custody judge authorises, for a period of one month, the installation of a surveillance tool — commonly referred to as a Trojan — developed by the *Gendarmerie*. The scope of this judicial authorisation remains somewhat ambiguous. It is unclear whether the decision pertained directly to the capture of data itself, which could not yet commence due to the need for prior technical preparations, or whether it merely authorised the execution of those preparatory operations. This uncertainty reflects broader inconsistencies in terminology between national and European judicial authorities when describing the digital investigative measure at stake.

12 February 2020
The liberty and custody judge extends the authorisation for an additional month, allowing continued installation of the Trojan.

4 March 2020
A further judicial decision permits the continuation of specific technical procedures necessary to support the functioning of the surveillance tool.

European Cooperation

2019

22 January / 19 and 21 February 2019
At the beginning of 2019, cooperation at the European level takes shape, recognising the cross-border scope of the EncroChat network and its users. Coordination meetings are held under the auspices of Europol, bringing together law enforcement representatives from France, the Netherlands, and the United Kingdom. These meetings lay the ground for a joint investigative strategy and the pooling of technical and legal expertise across jurisdictions.

2020

9 March 2020
During a videoconference organised by Eurojust, French and Dutch authorities inform several Member States of the data capture from the EncroChat network.

11 March 2020
The United Kingdom issues a European Investigation Order (EIO) seeking access to data from all EncroChat devices operating on UK territory.

13 March 2020
The German Federal Criminal Police Office (*Bundeskriminalamt*, BKA) initiates investigations against unidentified EncroChat users in Germany, primarily on suspicion of organised drug trafficking. Notably, the BKA considers the mere use of EncroChat devices sufficient to establish initial grounds for suspicion.

15 March 2020
A national investigative task force is established to coordinate the complex and multi-agency operation.

20 March 2020
The liberty and custody judge authorises the continuation of the technical operations.

20 March 2020
The Public Prosecutor's Office in Frankfurt formally opens urgent investigations targeting EncroChat users.

26 March 2020
The *Gendarmerie* presents its planned data processing framework to the French data protection authority (*Commission Nationale de l'Informatique et des Libertés*). This presentation includes a commitment to compliance with data protection standards and is accompanied by a technical dossier, which has remained confidential until today.

27 March 2020
Through Europol's Secure Information Exchange Network Application (SIENA), the French and Dutch authorities (leading the operation) requests that other EU national authorities formally acknowledge their awareness of the data collection methods and confirm their agreement that the incoming data would be used solely for analytical purposes at first.

31 March 2020
The liberty and custody judge issues a new authorisation concerning the technical deployment of the surveillance programme, specifying the measures required to ensure its lawful use.

31 March 2020
The United Kingdom's EIO of 11 March is authorised.

1 April 2020
Data begins to flow from EncroChat devices to French authorities. Investigators are immediately aware of the scale of the operation: approximately 66,000 users worldwide are affected, with around 32,000 active users, including roughly 4,600 in Germany and 380 in the United Kingdom.

10 April 2020
French and Dutch judicial authorities formalise their collaboration and sign an agreement for a Joint Investigation Team.

From April to June 2020
French authorities transmit raw data on a daily basis to Europol, which established a dedicated server to distribute country-specific datasets to participating Member States. The BKA retrieves daily data from Europol's servers concerning EncroChat users located in Germany from 3 April to 28 June 2020.

29 April 2020
The liberty and custody judge authorises a one-month extension of the data capture.

26 May 2020
The scope of the operation has become clear: the data capture encompassed 20,429 active devices across 122 countries, resulting in the collection of nearly 100 million messages in clear (not encrypted) and approximately 1,136 gigabytes of data. Within France, investigators have identified that 317 of the 454 active devices were being used for illicit purposes, while the remaining 154 showed little or no communications of evidentiary value.

28 May 2020
A judicial inquiry (*instruction*) is opened, based on a range of serious criminal charges. These included: conspiracy to commit crimes and offences punishable by at least ten years' imprisonment; drug trafficking; arms trafficking, money laundering; and the unauthorised provision, transfer, or importation of cryptographic devices without prior declaration.

The investigating judge, now in charge of the operations, authorises a four-month extension of the data capture operation.

2 June 2020
The Frankfurt Public Prosecutor's Office issues its first EIO to the French authorities, requesting unrestricted transmission and authorisation for the use of German-user data in domestic criminal proceedings. On 9 September 2020, a supplementary EIO is issued.

10 June 2020
The investigating judge issues a further authorisation to continue the technical measures necessary to support the ongoing surveillance and data collection efforts.

2 July 2021
The Frankfurt Public Prosecutor's Office submits a second supplementary EIO request, reflecting the ongoing need for access to EncroChat data as investigations expanded and deepened in Germany.

The scale and impact of the investigation became fully visible only after the operation. According to a press release issued by Eurojust in 2023, the operation led to the arrest of 6,558 individuals. Authorities seized, among others, over 100 tonnes of cocaine, 160 tonnes of cannabis, 923 weapons, 68 explosive devices, 271 properties, 83 boats, and 40 planes. In total, nearly €900 million in criminal assets were either seized or frozen, marking one of the most significant law enforcement operations against encrypted criminal communications networks in Europe.[5]

III. Complaints against the EncroChat Operation in France

Before outlining the litigation of the EncroChat operation before the French Court of Cassation, a brief introduction to the legal background of the data capture measure will provide the necessary context. We can also label this investigative measure as "legal hacking".

1. Legal background of the data capture measure

In French criminal procedure, data capture operations were introduced in 2011 under Articles 706-102-1 to 706-102-5 of the Code de procedure pénale (Criminal Procedure Code, CPC).[6] The general framework set out in Articles 706-95-11 to 706-95-19 CPC also applies. This legislation permits investigators, under judicial authorisation, to access, record, retain, and transmit various forms of digital data without the knowledge or consent of the targeted individuals. The scope of authorised data includes:[7]

- Visual data displayed on the user's screen, captured via screen-logging software;
- Keystrokes entered on the device, recorded through keyloggers;
- Audiovisual data transmitted through peripherals such as webcams or microphones, (though the data protection authority has explicitly prohibited remote activation of such devices[8]);
- Stored data — both content and metadata — accessed via backdoor mechanisms.

These operations may involve physical or remote installation of technical devices, including entry into private premises or vehicles, subject to strict judicial oversight. Authorisation may be granted either by the liberty and custody judge[9] during the preliminary investigation (for up to one month) at the request of the public prosecutor, or by the investigating judge during the judicial inquiry (for up to four months)[10]. The authorisation can be renewed but cannot exceed a total duration of two years. The authorisation must be made in

writing and state reasons, specifying the offence, the targeted system, and the duration of the operation. Operations are carried out under the authority of the authorising judge and may involve qualified agents from services under the Ministry of the Interior or Ministry of Defence. Detailed reports must be drawn up, including the timing and nature of the operations, and only data relevant to the authorised offences may be retained. Private life footage unrelated to the offences must be excluded from the case file. Recordings and data are sealed and ultimately destroyed upon expiry of the limitation period for prosecution. Article 706-102-5 CPC explicitly governs the conditions under which technical devices may be installed or removed, including entry into private premises outside legal hours, and transmission via electronic networks — all subject to judicial control.

2. Initial complaint before the Court of Cassation

The EncroChat case first reached the Court of Cassation in February 2022.[11] The defendants challenged the admissibility of the data gathered during the operation, arguing that the access to the clear (unencrypted) content had been made possible through technical means protected by national defence secrecy. Thus, the complaint did not directly address the legal framework governing the data capture itself, but rather focused on the decryption process. The use of such classified technical means is regulated under Articles 230-1 to 230-5 CPC. In effect, the defendants raised questions of a constitutional dimension, alleging that Articles 230-1 to 230-5 infringe upon the right to a fair trial and access to an effective remedy. Their arguments centred on two main points:

- The authorisation of the data capture measure by the public prosecutor, who is not considered an independent judicial authority in France due to their hierarchical subordination to the executive,[12] undermined judicial guarantees;
- When the technical methods used are classified under national secrecy, the defence is denied access to essential technical information, including the certificate signed by the head of the technical body "attesting the sincerity of the transmitted results" ("certifiant la sincérité des résultats transmis").[13]

The Court of Cassation deemed these concerns sufficiently serious and referred the legal questions to the Constitutional Council.

3. Decision by the Constitutional Council

In a brief eight-page decision issued in April 2022, the Constitutional Council dismissed said constitutional objections involving Articles 230-1 to 230-5 CPC.[14] The Council found that the procedural safeguards embedded in the legal framework for data capture sufficiently compensated for the limitations imposed by national secrecy. These safeguards include the requirement that data capture may only be authorised for a limited list of serious offences linked to organised crime; that the data must be sealed; and that the case file must contain a report on the installation of the technical device, as well as a description or transcription of the data deemed relevant to establishing the truth. Furthermore, all decrypted material must be accompanied by a certificate signed by the head of the technical body, attesting the "sincérité" ("sincerity") of the transmitted results. This is the only way under French law to testify that the data is correctly decrypted without omissions or tampering.[15]

Lastly, the Council noted that, if necessary, courts retain the power to request the declassification and disclosure of information protected by national defence secrecy, in accordance with the procedures set out in the Defence Code. On this basis, the Constitutional Council concluded that the legal framework does not violate the right to a fair trial.

In fact, the Constitutional Council's ruling means that there is in fact no transparency as regards the methods used, and this opacity is not subject to any specific legal framework. In other words, French law does not seek to regulate or limit the use of secret methods as such, as opposed to methods that are open or transparent.

4. Follow-up decisions by the Court of Cassation (2022)

After the legal battle before the Constitutional Council, the French Court of Cassation issued two significant decisions on the EncroChat case in October 2022.[16] In the first decision,[17] the Court mainly endorsed the Constitutional Council's reasoning; but also clarified other aspects.

One of the questions concerned the role of the certificate attesting the "sincerity" of the decrypted data (see above). In the first decision, the Court of cassation clarified that, in the decision challenging the admissibility of the evidence, the judge should not have disregarded this claim. In other words, the judge should have ruled whether the absence of the certificate was an issue. The decision also clarified the scope of the data capture under Article 706-102-1 CPC. The issue was whether the wording of the provision was limited to stored data, thereby excluding access to data in transit. Without truly ruling on the merits, the Court of Cassation clarified that the provision at issue does not distinguish between the forms of data — whether stored or in transit — and that there is therefore no need to address this question.

In its second decision,[18] the Court of Cassation addressed the legal implications of internal data transfers between separate investigations. In the case at issue, the original investigation in Lille had led to the opening of a case in a different city, i.e., Nancy. The defendant argued that he had been denied the opportunity to challenge the legality and fairness of the evidence originating from the Lille proceedings, as key documents had not been included in the Nancy case file. He claimed that this prevented him from verifying the quality and legality of the communication transcripts. The Court of Cassation rejected this argument, holding that the defendant had the right to request access to the original investigation file from the investigating judge (here: Lille) and to appeal any refusal.

In addition, the defendant questioned the integrity of the data, claiming that there was no proof that it had been properly sealed. The Court dismissed this claim as well, stating that procedural irregularities do not justify annulment unless the defendant can demonstrate actual prejudice.

The defendant finally sought to nullify the data capture on the grounds that it constituted an unfair investigative measure the result of which would be self-incrimination if a complaint were to be filed. The Court acknowledged that requiring a defendant to prove that they were affected by an irregularity, for example, by admitting their use of EncroChat – could infringe their right against self-incrimination. Therefore, it held that, in order to determine whether a person has standing to challenge the legality of a measure taken during an investigation, a defendant may either assert a personal interest in the matter or, where such an assertion would risk self-incrimination, the investigating chamber must assess the case file to determine whether the individual is potentially affected by the measure. As a result, even if a defendant denies using EncroChat, they retain standing to contest the legality of the evidence if the investigation attributes a device to them.[19]

5. Further decisions by the Court of Cassation (2023)

In 2023, the Court of Cassation issued two other brief decisions on EncroChat. In the first decision in February 2023,[20] the Court dismissed a challenge against the validity of one of the authorisations issued by the liberty and custody judge, arguing that it did not indicate a specified duration of the operation. According to the Court, a time limit is not required when the decision merely concerns "additional orders specifying the specific technical measures that must accompany the use of this device". This distinction, made by the Court, underscores a broader ambiguity in the legal framework: Does a judicial authorisation pertain to the data capture itself or to the technical operations accompanying it? The difference is not merely semantic, as each type of authorisation is subject to distinct procedural safeguards. The Court concluded that the data capture had been validly authorised by the liberty and custody judge on 30 January 2020, and that the one-month duration began only once the capture became technically operational, i.e., on 1 April 2020. This required no further judicial decision.

In its second decision in March 2023,[21] the Court of Cassation apparently contradicted the dominant narrative surrounding the EncroChat case to date, i.e., its focus on the potential illicit use of decryption techniques and the invocation of national defence secrecy. The defence relied on prior case law from both the Constitutional Council and the Court of Cassation interpreting Article 230-3 CPC, which requires that any decryption measure obtained through technical means be accompanied by sufficient technical information and a certificate attesting their sincerity (see also III.2. above). According to the defence, this requirement should have been respected in this case. Interestingly, the Court of Cassation held that Article 230-3 was inapplicable. After reviewing the case file, including elements not accessible to the defence, it asserted that the data had been captured and processed in clear form, and had never been accessed in an encrypted form. Consequently, no decryption had taken place. In this way, the Court effectively reclassified the case: Despite framing it as a matter of decryption and secrecy in public and legal discourse, the EncroChat operation was, in the Court's view, not an encryption case at all.

6. Scholars' reception

Most of the French academic criticism has focused on the ruling of the Constitutional Council (see above 2.).[22] A central concern is the opacity surrounding the technical means used to decrypt the data. Critics argue that this recourse to secrecy effectively removes key technical information from the adversarial process, undermining the principle of equality of arms. The absence of clear criteria or judicial oversight, either ex ante or ex post, over the classification of these methods is seen as granting prosecutors a level of discretionary power incompatible with guarantees of a fair trial. The Constitutional Council's justification for upholding this framework has been deemed inadequate, particularly given the potential for abuse and the lack of legal provisions explicitly protecting intelligence techniques from disclosure.

Beyond concerns about secrecy, the decision has also been criticised for its impact on defence rights. Defendants are unable to verify the origin or integrity of the data used

against them because they are denied access to the raw files and must rely solely on selected transcripts prepared by investigators. The procedural documents made available, such as the reasoned authorisations and reports on the installation and receipt of decrypted material, are considered inadequate for enabling meaningful scrutiny of the operation's legality and reliability.

The focus on the decision of the Constitutional Council, and consequently the focus on the use of secretive technological methods led most commentators, and the Court of Cassation itself, to overlook other essential issues. Consequently, some French scholars have noted that the legal and constitutional debates surrounding EncroChat in France have largely overlooked the core issue of the data capture operation itself. In particular, regarding the legality principle, given that such operations entail significant intrusion into private life, the legal framework authorising them should be "all the more clear and precise". Especially this point has been largely ignored by the Court of Cassation.[23]

IV. Complaints on the EncroChat Hacking before European Courts

1. EncroChat at the European Court of Justice

In the EncroChat case, the French authorities autonomously undertook the data capture; this meant that authorities in other Member States, such as the German authorities, were requesting data already in the possession of the French authorities. Thus, the EIOs issued were not requests for the execution of a data capture, but for the mere transfer of part of the stored data. This use of EncroChat data in criminal proceedings, obtained within the Joint Investigation Team and through EIOs, gave rise to significant legal controversy especially in Germany.[24]

In March 2022, the German Federal Court of Justice (Bundesgerichtshof) held that the Frankfurt Prosecutor's Office was competent to issue EIOs for the purpose of data transmission (a "transfer EIO") under the legal framework of the Directive regarding the European Investigation Order in criminal matters (EIO Directive),[25] and that the transferred data could be used as admissible evidence in criminal proceedings against individuals in Germany.[26] By contrast, the Regional Court of Berlin (Landgericht Berlin) questioned the admissibility of evidence for several reasons. The Berlin court found that only a judge (and not a prosecutor) should have issued the EIOs under the existing legal framework, given the seriousness of the interferences with fundamental rights and the absence of individualised suspicions. It further expressed doubts as to whether the EIOs complied with the requirements of necessity and proportionality, considering that the data collection had been broad, indiscriminate, and not linked to any specific case. Additional concerns were raised regarding the ability to challenge the integrity of the encrypted data (impossible to raise in France on grounds of "defence secrecy," see Section III) and regarding the notification obligations under Art. 31 of the EIO Directive. Ultimately, the Berlin court referred a comprehensive set of questions to the ECJ for a preliminary ruling.[27] On 30 April 2024, the ECJ delivered a landmark judgment interpreting the EIO Directive in the context of the EncroChat case.[28]

The questions referred to the ECJ essentially concerned the extent to which a Member State receiving data from another may review how the latter obtained such data. The Berlin Court raised questions about the conditions under which, (1) the data had been collected and (2) a "transfer EIO" could legitimately be issued. As the EIO Directive refers mostly to national law, it imposes few substantive safeguards. The questions referred to the ECJ were largely intended to highlight the absence of stronger guarantees under EU law.

Looking at the first question concerning the authority competent to issue a "transfer-EIO", it is important to note that, under German criminal procedural law, only a judge may order a legal hacking measure as that carried out in France. However, the ECJ departed from the approach, holding that the EIO did not need to be issued by a judge, on the ground that the "transfer EIO" merely sought the transmission of data already collected by the French authorities. In the absence of mandatory judicial authorisation for such transfer between two criminal proceedings at the national level, the EIO could thus be issued by a prosecutor.

With regard to the second question, the Berlin court enquired whether safeguards related to its own provisions on legal hacking, such as the need for an individualised suspicion against the persons targeted by the investigation, and whether the verification of data integrity apply, given that both safeguards are not explicitly provided for in the regulation of legal hacking in France. However, the ECJ barred the issuing state from requiring such safeguards. The ECJ stressed again that the EIO related to the mere transfer of data, not the implementation of legal hacking. Furthermore, as the EIO Directive does not prescribe such requirements, the ECJ declined to create new safeguards.

Nevertheless, the ECJ opened the door to a limited review by the issuing state: Where a "transfer-EIO" appears disproportionate in light of the fundamental rights of the persons

concerned, "the court seized of the action brought against the EIO ordering that transmission would have to draw the appropriate conclusions from this as required under national law".[29] In this context, the ECJ referred to Art. 14(7) EIO Directive, according to which rights of the defence and the fairness of proceedings must be upheld, particularly by providing the opportunity to effectively comment on the evidence. If national courts consider these rights to have been violated, data resulting from a "transfer-EIO" can be rendered inadmissible.[30] However, this possibility remains confined to the domestic legal order.

Finally, the ECJ determined the meaning of "interception of telecommunications" as set out in Arts. 30 and 31 EIO Directive. The Court transformed the notion into an autonomous concept of EU law, independent of national definitions. Here, the ECJ interprets the word "interception" broadly, including any infiltration of devices for the purpose of gathering communication data, even internet-based data. As a consequence, interception not only includes the interception of data in transit, but also the mere gathering of stored data, as in the EncroChat case. Hence, if the subject of the operation is located in another Member State, the state from which the interception originates (here: France) must notify each state in which users are located. This notification, deriving from Art. 31 EIO Directive, enables the notified state to request the termination of the measure or to impose conditions, such as additional safeguards, necessary for evidence to be admissible in later proceedings.

Thus, the ECJ largely left significant questions, and particularly the one as to the admissibility of the evidence, entirely to national law and courts. While the German courts seemed wary of the conditions under which the legal hacking took place in France, the ECJ refocused the case in direction of the provisions surrounding the data transfer between criminal proceedings. The ECJ's decision has triggered ample literature from different perspectives, namely EU law, fundamental rights and technical guarantees.[31] Conversely, to our knowledge, the ECtHR's decision, which we will discuss next, remains largely absent from the debate.

2. EncroChat at the European Court of Human Rights

The ECtHR also had the opportunity to rule on the EncroChat case.[32] In this particular instance, the applicants were prosecuted in the United Kingdom. The British authorities had relied on data transferred by the French authorities following a corresponding EIO. Notably, the application before the ECtHR was lodged against France, which collected and transferred the data, rather than against the United Kingdom, which used this data in domestic criminal proceedings. The applicants alleged that France violated their right to privacy, their right to a fair trial, and their right to an effective remedy (Arts. 8, 6 and 13 ECHR). Two specific interferences were at stake:

- The initial collection of data;
- The transfer of the data, with the applicants arguing that the large-scale transmission of data to the United Kingdom constituted a separate violation of their fundamental rights.

The ECtHR declared the application inadmissible, however, and did not examine the merits of the case because domestic remedies had not yet been exhausted (principle of subsidiarity). The Court accepted the French government's argument that the applicants should have used the effective remedies available to them in France before bringing their case to Strasbourg. Notably, reference was made to Article 694-41 CPC, which provides that remedies must be available in France against measures executed pursuant to an EIO whenever similar remedies exist in domestic law for comparable internal measures. In the case at hand, the reference point was the transfer of data already collected from one case file to another, as also highlighted by the ECJ and labelled above as the "transfer-EIO". Although the French criminal procedure code does not expressly provide for a remedy against data transfers, the Court of Cassation has recognised the possibility of an annulment claim (recours en nullité) against data transfers between national criminal proceedings within France.[33]

The ECtHR's reasoning is open to two criticisms. The first concerns the accessibility of the remedy: It is far from evident that foreign applicants could reasonably be expected to identify the procedural avenues available under French law without assistance or notification of the collection of their EncroChat data. Secondly, even if such information were accessible, it is uncertain whether the French courts would recognise the applicants' claims, given that they were not directly involved in any criminal proceedings in France. It should be noted that the legal question of access to such remedies is currently being debated in the SkyECC proceedings, another cryptophone case (see Section VI.).

By accepting the inadmissibility argument, the ECtHR missed an opportunity to analyse a measure of legal hacking for the first time. Yet, as the Court itself highlights in para. 102 of the decision, the analysis and use of bulk data as evidence, whether resulting directly from legal hacking or from a transfer of the collected data, qualify as "undoubtedly being the most intrusive [steps] in the process"[34] but these acts were "not among those brought before the Court."[35] Therefore, there is hope that the Strasbourg Court

will have the opportunity to revisit the fundamental rights issues in substance, particularly the right to privacy, the proportionality of analysing bulk data in view of the limited safeguards regarding legal hacking (in France), and the proportionality of the data transfer to many other countries.

V. New Complaints on the EncroChat Hacking in France (2025)

Following the ECJ's and ECtHR's decisions, the Court of Cassation issued four decisions related to the EncroChat data capture during the first quarter of 2025.

In January 2025, the Court reaffirmed that circumventing EncroChat's "infrastructure protection system" had allowed investigators to access "the data itself, which was readable in plain text within the files."[36] This means that the data collected was never encrypted and later decrypted by the investigators, as had been already stressed by the Court in its May 2023 decision (see above, section III.5). The Court also reiterated that judicial authorisations concerning the installation of technical measures do not require a time limit, and are not subject to "specific technical requirements." This position in effect excludes judicial authorisations for future data capture from the enhanced safeguards applicable to technical means protected by national defence secrecy.

Despite this limitation, the Court proceeded to assess the proportionality of the data capture operation in light of the ECJ's case law on indiscriminate data retention and access.[37] It concluded that the operation was sufficiently targeted, as authorisation had to be obtained for specific automated data processing systems, such as servers identified by their IP addresses and the terminals and peripherals connected to them. As the measure was limited to EncroChat users (even if all of them), the Court held that it did not constitute mass surveillance. In our view, the Court's analysis reflects a narrow interpretation of the ECJ's data retention case law, which cannot be fully explored in this article. At least, the Court acknowledged a technical safeguard by requiring installation reports for the capture devices to be included in the case file. Importantly, in this context, it clarified that it is the responsibility of the investigating judge, rather than the defendant, to request these reports.

In two subsequent decisions issued in February 2025,[38] the Court of Cassation addressed the procedural safeguards and remedies available to defendants in the context of data capture. As a general rule, individuals may challenge the legality of investigative measures taken prior to their formal indictment within six months of being notified of the indictment (Article 173-1 CPC). This time limit does not apply, however, if the contested operations were not already included in the case file. In the EncroChat proceedings, the data capture was only added to the case file after the defendants had been charged. Against this backdrop, the Court held that it would be unlawful to refuse judicial review of the measure in such cases. Instead, the six-month time limit for contesting the legality of the operation must begin from the date of the defendant's interrogation after the addition of the data capture reports to the case file.

Finally, in March 2025,[39] the Court of Cassation revisited the principle of the right against self-incrimination. In the case at hand, the investigating chamber rejected an appeal challenging the legality of the data capture on the basis that the defendant had denied being an EncroChat user. However, the Court of Cassation overturned this reasoning, reaffirming its 2023 case law: A defendant is not required to admit ownership or use of the cryptophone in order to access remedies. Conversely, it is the responsibility of the courts to establish whether the individual is connected to the device under investigation. If the prosecution establishes such a connection, the defendant must be granted access to legal remedy in order to challenge the legality of the data capture.

VI. Potential Next Steps

Although the EncroChat case has attracted considerable attention, the French and European litigation concerning the measures implemented in France remain unsatisfactory in several respects. In particular, the French courts have not fully examined whether legal hacking was necessary and proportionate. This shortcoming may be due to several factors: the novelty, complexity, and sensitivity of the case; as well as procedural choices shifting the debate towards highly technical matters to the detriment of fundamental questions.

At the European level, neither the ECJ nor the ECtHR has yet addressed the substance of the proportionality of the legal hacking carried out in France. They also have not dealt with the implications of these measures for criminal proceedings abroad. Several applications are pending before the ECtHR, which will likely offer the opportunity to revisit the matter. However, as these applications are not directed against France as the "collecting country", the Court in Strasbourg is not going to discuss the proportionality of legal hacking.[40]

Ultimately, EncroChat is no longer an isolated case. Similar questions have emerged in other cryptophone proceedings,

most notably in the SkyECC case. This case extends the debate to the crucial issue of whether individuals whose data were collected on French territory but used against them abroad can access remedies in France (see above, section IV.2). Under current French law, such individuals may be denied redress and therefore have no access to domestic remedies. In the SkyECC case, the French Court of Cassation has refused to refer this issue to the Constitutional Council,[41] but instead requested a preliminary ruling from the ECJ.[42] This situation has already given rise to numerous issues concerning the admissibility of evidence in various European countries, which will need to be addressed separately. This is a different story to tell.

Pending these legal and technical challenges, the judicial chronology of data-driven investigations is still unfolding.

Dr. Maxime Lassalle-Han
Maître de Conférence, Law Faculty,
Burgundy University, France

Dr. Salomé Lannier
Post-doctoral researcher, FDEF,
University of Luxembourg

1 J.-J. Oerlemans and S. Royer, "The future of data driven investigations in light of the Sky ECC operation", (2023) 14(4) *New Journal of European Criminal Law*, 434–458.
2 Europol Press Release of 3 December 2024, "International operation takes down another encrypted messaging service used by criminals –<https://www.europol.europa.eu/media-press/newsroom/news/international-operation-takes-down-another-encrypted-messaging-service-used-criminals>. All hyperlinks in this article were last accessed on 8 April 2026. See also C. Riehle and T. Wahl, "Trojan-Encrypted Device Reveals Criminal Activities", (2021) *eucrim*, 106.
3 The *Cour de cassation* (Court of cassation) is the highest court in the French judiciary. It has jurisdiction to hear cases in civil, commercial, social or criminal matters. The Court only reviews questions of law (but not questions of fact) and bears ultimate responsibility for a uniform interpretation and application of statutory law throughout France. It also filters out appeals challenging the constitutionality of statutes before forwarding them to the *Conseil constitutionnel* (Constitutional Council).
4 This chronology is based on dates extracted from the following documents: C. Thorfinn, "L'enquête EncroChat en France – Genèse du dossier et chronologie de la procédure EncroChat", *Policy Commons*, 2 July 2020, <https://policycommons.net/artifacts/1918483/lenquete-encrochat-en-france/2670254/> ; ECtHR, 24 September 2024, *A.L. et E.J. v. France (dec.)*, Appl. nos. 44715/20 and 47930/21; ECJ, 30 April 2024, Case C-670/22 , *Criminal proceedings against M.N. [Encrochat]*; Eurojust, *Annual Report 2020: Criminal justice across borders in the EU*, 23 March 2021, <https://www.eurojust.europa.eu/sites/default/files/assets/2021_04_14_eurojust_annual_report_2020_final.pdf>; Europol, *Internet organised crime threat assessment (IOCTA) 2020*, <https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf>; Cour de cassation, Chambre criminelle, 14 February 2023, 22-84.288.
5 Eurojust Press Release of 27 June 2023, "Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized", , <https://www.eurojust.europa.eu/news/dismantling-encrypted-criminal-encrochat-communications-6-500-arrests-900-eur-seized>; see also C. Riehle, "Results of EncroChat Take-Down", (2023) *eucrim*, 163–164.
6 Law no. 2011-267 of 14 March 2011 on guidelines and planning for internal security performance (*loi n. 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure*).
7 B. Roussel, *Les investigations numériques en procédure pénale*, PhD thesis, Université de Bordeaux, 7 July 2020, pp. 199–200, online <https://theses.hal.science/tel-02947825>; M. Quéméner, "Fasc. 1105 : La preuve numérique dans un cadre pénal", *JurisClasseur Communication*, LexisNexis, 8 November 2022 ; E. De Marco, "La captation des données", in: K. Blay-Grabarczyk et al. (eds.), *Le nouveau cadre législatif de la lutte contre le terrorisme à l'épreuve des droits fondamentaux*, Institut Universitaire Varenne, Collection "Colloques & Essais", no. 44, 2017, p. 88.
8 CNIL, *Délibération portant avis sur un projet de décret modifiant le décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale*, September 2019, demande d'avis n°18004354.
9 The liberty and custody judge is a judicial authority responsible for authorising intrusive investigative measures during a preliminary investigation. They perform a role similar to that of an investigating judge (*juge d'instruction*), but specifically in the context of safeguarding individual liberties prior to the opening of a formal judicial inquiry (*instruction*).
10 The authority responsible for granting the authorisation will depend on the framework of the investigation.
11 Cour de cassation, Chambre criminelle, 1 February 2022, 21-85.148. The same issues reached the Court again in April 2022: Cour de cassation, Chambre criminelle, 5 April 2022, 21-85.763.
12 ECtHR, 23 November 2010, *Moulin v. France*, Appl. no. 37104/06.
13 Article 230-3 CPC whose crucial passage reads: « Sous réserve des obligations découlant du secret de la défense nationale, les résultats sont accompagnés des indications techniques utiles à la

compréhension et à leur exploitation ainsi que d'une attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis. »

14 Conseil constitutionnel, 4 April 2022, *M. Saïd Z.*, no. 2022-987 QPC.

15 However, the Constitutional Council did not address the meaning of the "sincerity" requirement. Indeed, the concept of "sincerity" is not used elsewhere in the legal framework, neither in the criminal procedure code nor in the Law no. 78-17 of 6 January 1978 "on information technology, files and civil liberties" (*Loi n. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*.). The latter was, *inter alia*, amended to transpose the EU's 2016 Law Enforcement Directive (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, OJ L 119, 4.5.2016, 89). On the one hand, the concept could mean that the results, i.e., the selection from the raw data, must be certified sincerely, as not to exclude exculpatory evidence. On the other hand, and on a different note, "sincerity of the results" could refer to the integrity or authenticity of the data from a forensic perspective.

16 For an analysis in the French literature, see J. Pidoux, "Nullités en matière de captation de données informatiques : précision et rappel sur la qualité à agir du requérant Crim. 25 oct. 2022, FS-B, n. 21-85.763", *Dalloz Actualité*, Dalloz, 15 November 2022 ; J. Pidoux, "Premiers contrôles par la Cour de cassation de procédures ouvertes à la suite de l'opération dite « EncroChat » Crim. 11 oct. 2022, F-D, n. 21-85.148 Crim. 25 oct. 2022, FS-B, n. 21-85.763", *Dalloz Actualité*, Dalloz, 14 November 2022.

17 Cour de cassation, Chambre criminelle, 11 October 2022, 21-85148.

18 Cour de cassation, Chambre criminelle, 25 October 2022, 21-85.763.

19 The ECtHR relied particularly on this decision when assessing the existence of a remedy in France against legal hacking (see Section III.2), ECtHR, *A.L. et E.J. v. France (dec.)*, *op. cit.* (n. 4), § 141.

20 Cour de cassation, Chambre criminelle, 14 February 2023, *op. cit.* (n. 4).

21 Cour de cassation, Chambre criminelle, 10 May 2023, 22-84.475.

22 C. Ascione Le Dréau, "QPC dans l'affaire EncroChat : des jours heureux pour Big Brother ? Décision rendue par Conseil constitutionnel", *Actualité juridique Pénal*, Dalloz, 2022, p. 376 ; X. Laurent, "Captation de données numériques : une étape significative dans la consolidation du régime de l'article 706-102-1 du code de procédure pénale", *Dalloz IP/IT*, Dalloz, 2022, p. 578 ; M. Lassalle, "L'affaire EncroChat", *Recueil Dalloz*, Dalloz, 2023, p. 1833 ; L. Saenko, "Captation de données informatiques et secret-défense : une arme sans contrôle ?", *Lexbase* pénal, 2022, no. 48.

23 M. Lassalle, "L'affaire EncroChat", *op. cit.* (n. 22), p. 1833.

24 See T. Wahl, "EncroChat Turns into a Case for the CJEU", (2022) *eucrim*, 197–198. In this part on the EncroChat case before the ECJ, we exclude the following ECJ order from our analysis, as it does not concern the French procedure: ECJ, 4 July 2024, Case C-288/24, *Criminal proceedings against M.R.* For this decision, see T. Wahl, "Berlin Regional Court's EncroChat Battle – Third Round, (2024) *eucrim*, 86–87.

25 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, 1.

26 For a summary of this decision in English, see T. Wahl, "Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases", (2022) *eucrim*, 36–37.

27 T. Wahl, (2022) *eucrim*, *op. cit.* (n. 24), 197–198.

28 ECJ, *Criminal proceedings against M.N. [Encrochat]*, *op. cit.* (n. 4). For the summary of this judgment in eucrim: T. Wahl, "ECJ Ruled in EncroChat Case", (2024) *eucrim*, 40–43.

29 ECJ, *Criminal proceedings against M.N. [Encrochat]*, *op. cit.* (n. 4), para. 103.

30 ECJ, *Criminal proceedings against M.N. [Encrochat]*, *op. cit.* (n. 4), paras. 104–105. On this aspect, the ECJ relied on its previous case law, ECJ, 2 March 2021, Case C-746/18, *Criminal proceedings against H K vs Prokuratuur*.

31 See L. Bachmaier Winter, "The fight for fair trial rights and the paradigm shift in evidence: from liberalism to mass surveillance in criminal proceedings in Europe", (2025) 11(1) *Revista Brasileira de Direito Processual Penal*; S. Steinborn and D. Swieczkowski, "Verification in the Issuing State of Evidence Obtained on the Basis of the European Investigation Order", (2023) 54 *Rev. Eur. & Comp. L.*, 169–194 ; A. Sachoulidou, "The Court of Justice in *Staatsanwaltschaft Berlin v. M.N.* (EncroChat): From cross-border, data-driven police investigations to evidence admissibility", (2024) 31(4) *Maastricht Journal of European and Comparative Law*, 510–520; M. Nicolas-Gréciano, "Affaire EncroChat devant la CJUE : premiers accrocs aux droits fondamentaux", *La Gazette du Palais*, 9 July 2024, vol. 23, 18–21 ; M. Lassalle, "La phase supranationale de l'affaire EncroChat", *Recueil Dalloz*, 3 July 2025, p. 1194 ; A. Hoxhaj, "The CJEU Ruled that the EncroChat Data can be Admissible Evidence in the EU", (2025) 16 *European Journal of Risk Regulation,* 1567–1579; A. Caiola, "Un arrêt fondateur entre efficacité et protection des droits. La décision d'enquête européenne en matière pénale et quelques précisions jurisprudentielles sur la transmission et l'utilisation de preuves", (2024)(2) *Law & European Affairs*, 341–352; V. Bajović and V. Ćorić, "Encrochat and SkyECC Data as Evidence in Criminal Proceedings in Light of the CJEU Decision", (2025) 33 *European Journal of Crime, Criminal Law and Criminal Justice*, 235–262.

32 ECtHR, *A.L. et E.J. c. France (dec.)*, *op. cit.* (n. 4).

33 ECtHR, *A.L. et E.J. c. France (dec.)*, *op. cit.* (n. 4), para. 82. Cour de cassation, Chambre criminelle, 25 octobre 2022, 21-85.763.

34 Referring to ECtHR, 25 May 2021, *Big Brother Watch and Others v. the United Kingdom*, Appl. nos. 58170/13, 62322/14, 24960/15.

35 The translation is made by the authors from the official French text of the decision.

36 Cour de cassation, Chambre criminelle, 7 January 2025, 24-82.908.

37 See for instance: ECJ, 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*; ECJ, 6 October 2020, Joined Cases C-511/18, C-512/18, and C-520/18, *La Quadrature du Net and Others*; ECJ, 5 April 2022, Case C-140/20, *G.D. v. Commissioner of An Garda Síochána*; ECJ, 20 September 2022, Joined Cases C-793/19 and C-794/19, *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH*; ECJ, 30 April 2024, Case C-470/21, *La Quadrature du Net and Others v Premier ministre and Ministère de la Culture*.

38 Cour de cassation, Chambre criminelle, 4 February 2025, 24-80.567; Cour de cassation, Chambre criminelle, 4 February 2025, 24-80.411.

39 Cour de cassation, Chambre criminelle, 26 March 2025, 21-83.122 & 23-87.113.

40 Joint Defense Team, "Update 2025: EncroChat and SkyECC Legal Developments Across Europe"30 October 2025, <https://www.joint-defense-team.com/post/encrochat-skyecc-legal-update-2025>.

41 Cour de cassation, Chambre criminelle, 3 June 2025, 25-80.792 ; Cour de cassation, Chambre criminelle, 3 June 2025, 25-80.497. See also Cour de cassation, Chambre criminelle, 18 November 2025, 25-82.065 ; Cour de cassation, Chambre criminelle, 31 March 2026, 25-82.068.

42 Cour de cassation, Chambre criminelle, 16 September 2025, 24-84.262 (referenced at the ECJ as Case C-625/25, "*Prudniez*").

What Remains of the *ordre public* in Transnational Surveillance?

A Commentary on the Decisions of the Federal Court of Justice and the Federal Constitutional Court in the ANOM Proceedings

Thomas Wahl*

ANOM was an undercover law enforcement operation in which the American FBI distributed encrypted mobile phones with a hidden backdoor, allowing authorities to monitor previously untraceable criminals' communication in real time. Many details of the operation were kept confidential by law enforcement. The intelligence gathered led to hundreds of arrests worldwide, major drug seizures, and disruption of organised crime networks.
Continuing the discussion initiated by *Lassalle* and *Lannier* (in this issue), who retrace the EncroChat police operation in France, this article analyses two rulings by Germany's highest courts (the Federal Court of Justice and the Federal Constitutional Court) that approved the use of chat data obtained from the ANOM operation. Despite many differences between EncroChat and ANOM, both courts saw no reason to depart from the evidence-friendly case law they had each already established in the German EncroChat cases. The author argues that the approach adopted by the courts with regard to the public order (*ordre public*) under mutual legal assistance law does not do justice to the subject matter in ANOM and that statements against the admissibility of evidence should have been made.

I. Introduction

The same legal outcome was reached in two criminal proceedings involving the ANOM operation, despite technical and legal differences in the collection of evidence from cryptophones. This is the main conclusion in both the decision of the German Federal Court of Justice (FCJ, *Bundesgerichtshof*) on 9 January 2025[1] and that of the Federal Constitutional Court (FCC, *Bundesverfassungsgericht*) on 23 September 2025.[2] Both courts held that evidence obtained via the decryption and surveillance of chat messages on ANOM devices was admissible in criminal proceedings against "German users". Both courts essentially followed the line of argumentation they had developed in the EncroChat case and later applied to the SkyECC case,[3] which also dealt with the admissibility of evidence of criminal activity obtained by investigators via the infiltration of encrypted mobile phones. However, the ANOM operation is unique in that it was not carried out by police authorities in EU countries, but by the U.S. Federal Bureau of Investigation (FBI), and much of the background to the operation has been deliberately kept obscure.

Having spoken out almost unanimously in favour of a ban on the use and exploitation of data obtained from abroad in the EncroChat and SkyECC proceedings, German legal scholars reinforced their position in the ANOM cases. In this context, a ban has been primarily derived from constitutional law, European law, and on domestic criminal procedural grounds.[4] This article contributes to the discussion by focusing on the legal basis for mutual legal assistance (MLA) in the two German decisions and by taking a closer look at the courts' arguments based on "*ordre public*".

Section II summarises the facts underlying the two decisions. Section III then outlines the main reasons given by the FCJ and the FCC in their decisions. Section IV comments on the judicial arguments, focusing on the reasoning behind the "*ordre public*" exception, before conclusions are drawn in Section V.

II. The ANOM Case: Facts, Background, and Legal Question

The FCJ and the FCC based their decisions on the following facts:[5]

Following an investigation by US authorities into a company that sold cryptophones to members of criminal organisations for the purpose of encrypted communication, the FBI developed "ANOM" cryptophones to sell to these organisations. Although each ANOM device was end-to-end encrypted, the FBI was, unbeknownst to users, in possession of the codes enabling each sent message to be decrypted. Since the summer of 2019, the iBot server, which received a copy of each sent message, was located in "an EU Member State". The FBI first decrypted the messages in temporary

storage on that server, then re-encrypted them, and finally forwarded them to the transfer server with a few days' delay. This enabled the communication of ANOM users to be continuously monitored.

In October 2019, a court order was issued in said EU Member State which enabled a copy of the server to be made and its content to be received by the US authorities until June 2021, in accordance with a bilateral mutual legal assistance treaty between that EU Member State and the United States. At the country's request, the FBI did not reveal the identity of the EU Member State, and it is not known why this EU Member State requested secrecy in this matter. The content of the court order(s) allowing the recovery and transmission of the data has also not been disclosed.

In September 2020, the German Federal Criminal Police Office (*Bundeskriminalamt*, BKA) was granted access to the decrypted content data for information purposes, with a link to Germany via an internet-based analysis platform. On 31 March 2021, the Frankfurt am Main General Public Prosecutor's Office (*Generalstaatsanwaltschaft Frankfurt am Main*) initiated proceedings against the users of ANOM cryptophones. On 21 April 2021, the Office submitted a request for mutual legal assistance to the U.S. Department of Justice, which consented to the use of the transmitted data in a letter dated 3 June 2021. It clarified, however, that the FBI would not provide support for the criminal proceedings in Germany, including witness testimonies or the authentication of documents.

German public prosecution services subsequently conducted individual criminal proceedings against users of ANOM devices in Germany, most of which concerned drug trafficking and the proliferation of weapons. Criminal courts convicted the individuals, the decrypted chat messages exchanged via the ANOM devices regularly being the only supporting evidence.

The defendants argued that Sec. 261 of the German Code of Criminal Procedure (*Strafprozessordnung*, StPO), which is the constitutional basis for the admissibility of evidence presented at trial in Germany, had been violated and that the evidence had to be excluded. The reasoning was that, unlike in the EncroChat case, the court order(s) was/were not known ("orders from hearsay"), and a verification on the basis of rule-of-law standards has been impossible. They also argued that, regardless of any concrete grounds for suspicion, the FBI had engaged in abusive "forum shopping", which the German law enforcement authorities adopted as their own and thus continued the abusiveness.

Overall, it can be noted that the ANOM and EncroChat/SkyECC operations have little in common. In both cases, the main focus was on monitoring a private telecommunications server via infiltration software. Information initially came to Germany through police channels, and the use of the data was subsequently approved through judicial assistance.[6] There are some striking differences between the operations however.[7] In contrast to EncroChat/SkyECC, ANOM is characterised by:

- Mobile phones (cryptophones), developed by the state (USA) and distributed under the control of police forces (the FBI) using front companies;
- Investigators being able to read seemingly fully encrypted messages at any time thanks to their own decryption codes;
- Unclear reasons for the secrecy surrounding the geographical outsourcing of the evidence collection (to an unknown state hosting the server in the EU) and the content of the court surveillance orders, due to the FBI's confidentiality agreement.

III. The Reasoning

1. The FCJ's main line of argumentation

In its judgment of 9 January 2025, the FCJ first reiterated the main principles for the use of evidence collected in a foreign legal order and the German approach to exclusionary rules:

- A prohibition against the use of evidence is an exception that requires justification, given that the primary objective of criminal proceedings is to reach a just and materially correct decision;
- The admissibility of evidence obtained through mutual legal assistance (MLA) shall be governed by the law of the requesting state (*lex fori*);
- The legality of investigative measures in the requested state shall not be reviewed against the standards of the requesting state's legal system;
- In international cooperation in criminal matters, it is rather necessary to respect the structures and content of foreign legal systems and views, even if they do not correspond in detail to domestic – in this case, German – views; otherwise, the sovereignty of the other state would be called into question;
- Mere non-compliance with German law in a foreign investigation does not in itself constitute grounds for a (dependent) prohibition on the use of evidence;
- The inadmissibility of evidence may result from a violation of the principles of national and European ordre public (Section 73, sentence 1 IRG8) or guarantees of

binding international law with individual legal protection – such as Art. 3 of the European Convention on Human Rights (ECHR) – during the collection of evidence.

With regard to the case at issue, the FCJ further examined the consequences of a potential violation of Art. 31 para. 1 of the Directive regarding the European Investigation Order (i.e., the failure to notify an EU Member State on whose territory an interception order is used and from which no technical assistance is needed to carry out the interception). According to the FCJ, a violation by the "unknown third state party which is an EU Member State" (i.e., the state hosting the server) of the notification obligations does not lead to the exclusion of evidence, as the state's interest in investigating the case outweighs the defendant's right to privacy and communication.

The following main part of the FCJ's judgment was dedicated to the findings of a possible violation of the *ordre public*, which the FCJ rejected by arguing as follows:

- A lack of knowledge regarding both the identity of the monitoring third country and the content of the decisions taken there does not constitute a violation of fundamental principles of the rule of law. The reason for this is because the principle of mutual trust requires that the legality of official acts and investigative measures carried out abroad be assumed at first. This principle also applies to mutual legal assistance with the USA. Only if there are reliable indications that the requested state has not acted in accordance with the law can the presumption of lawful action be refuted. Such non-lawful conduct does not arise specifically from the FBI's failure to disclose information, as confidentiality commitments and source protection are not foreign to German criminal proceedings either. Investigative measures do not have to be completely transparent.
- The FBI operation was not a groundless mass investigation and mass data analysis and thus essentially a secret service measure for which there would be no legal basis in criminal proceedings.
- Since this was not a case of indiscriminate mass surveillance, intercepting ANOM data was not disproportionate, but rather a permissible criminal investigation tactic (zulässige kriminalistische List).
- The essence of the German and European principle of a fair trial was not violated, since the proceedings as a whole were not unfair. The requirements of a functioning criminal justice system must also be taken into account in this context.
- In addition, the minimum standards of the rule of law were not violated by the defendant not having had the opportunity to have the orders reviewed by a court. Although the lack of primary legal remedies deprives the defendant of legal protection, this does not affect the essence of the relevant fundamental rights (telecommunications secrecy and the general right of personality), either institutionally or individually (through the use of the ANOM findings). The German Code of Criminal Procedure also provides for comparable measures with regard to telecommunications surveillance in Sec. 100a StPO.

2. The FCC's main line of argumentation

In its order (*Beschluss*) of 23 September 2025, the FCC essentially shared the FCJ's argumentation and approach, particularly with regard to the exceptional character of accepting evidential exclusionary rules in German criminal procedure, the principal non-review of the sovereign decisions of the requested state against the standard of the requesting state's law, and the general adherence to the structures and substantive content of foreign legal orders and perspectives, even if they are not necessarily consistent with domestic views in an individual case.

The Federal Constitutional Court also emphasised the importance of the principle of mutual trust in international cooperation in criminal matters, which leads to the "as-long-as" formula: It must be assumed that principles of the rule of law and human rights protection have been observed in the foreign state, as long as this is not refuted by the facts of the case. In the present case, there were no indications that suggested an undermining of mutual trust, according to the FCC.

Among other things, the FCC highlighted two aspects of the case that supplement the FCJ's ruling:

- Lack of knowledge regarding the unknown EU country hosting the server is irrelevant, as the legality of the collection procedure is fundamentally irrelevant to the usability of the data. Furthermore, the manner of collection and the maximum scope (= users of the devices) were limited, as specified by the FBI.
- The argument that there were insufficient opportunities to influence the course and outcome of the proceedings is invalid, because the complainant could have commented on the communications surveillance affecting him and, in particular, called into question the authenticity of these communications in the German proceedings. Even if the lack of influence in the unknown EU state were considered deficient and questionable from a constitutional point of view, this would be irrelevant here, because the collection of evidence in the requested state is insignificant for the question of the prohibition of evidence in the *lex fori*, as laid out above.

IV. Commentary

The ANOM operation did not lead the FCJ and FCC to deviate from the approach taken in the EncroChat/SkyECC proceedings. This outcome has been achieved primarily through adherence to the traditional approach of applying the "*forum regit actum*" principle to the question of the use of evidence collected abroad, negating the need for legality control of measures taken in the "surveilling state", and placing a strong emphasis on the maxim of mutual trust that governs international cooperation in criminal matters. The FCJ and FCC rulings have met with fierce opposition in the German legal literature. Above all, scholars have criticised the defendant's inability to obtain sufficient legal protection, the disproportionality of the operation in placing all purchasers of the mobile phones under general suspicion, and the failure to follow up on concrete indications of forum shopping.[9] The discussion in the next subsections will be guided by three key questions, viewed through the lens of mutual legal assistance (MLA):

- Is the approach of applying the *forum regit actum* principle to all questions regarding the use of foreign evidence still up to date in the present context?
- What is the yardstick for an *ordre public* assessment (national or European)?
- What arguments can be raised against the courts' findings with regard to the *ordre public* in the ANOM case?

1. The *lex fori*-approach – Still up to date?

This subsection examines whether, in transnational surveillance police operations such as those in ANOM (and also in EncroChat), the "preliminary question" – assessing foreign evidence under the *lex fori* standard, coupled with the factual exclusion of reviewing the legality of the measure in the "requested state" – can still be followed.

The German courts' statement that the admissibility of evidence obtained through MLA is governed exclusively by the national law of the requesting state (*lex fori*), combined with the statement that the sovereign decisions of the requested state are not, in principle, subject to review under the standards of the requesting state's legal system,[10] appears irrefutable. However, it should be noted that this maxim was developed in "traditional" MLA situations, those in which German judicial authorities issued a request for a specific investigative measure to a foreign state, which then executed the measure.[11] In these situations, the German judicial authorities at least had the opportunity to influence the investigative measure in the foreign state (including the possibility of asking for "German" safeguards in accordance with the *forum regit actum principle*[12]). At the later trial stage, it was possible to review whether procedural flaws that did not comply with German criminal procedure order had consequences on the use of the evidence collected abroad.[13]

Departing from this concept, the EncroChat case and, even more strikingly, the ANOM case each reveal a completely different scenario: A foreign police force conducted investigations into an initially undefined number of persons, thereby encroaching upon their fundamental right to privacy through surveillance measures (using infiltration techniques), and then distributed the "final product" (data collected on users in other countries) to police forces in other territories for their use. Judicial authorities in these territories were hardly, if at all, involved in these law enforcement operations from the outset, and the evidence was primarily transmitted through police channels. Only retrospectively was an MLA request submitted by the judicial authorities – purely as a formality – in order to have the authorisation for use rubber-stamped.

The courts' statement that "evidence was obtained '*by way of mutual legal assistance*'" must be viewed with considerable scepticism. Most notably, the courts failed to address fundamental issues, including the completely different quality of information gathering compared to previous MLA practice, the relationship between police assistance and judicial assistance, and the consequences arising from this. By separating the state *gathering* evidence from the state *utilising* evidence, the FCJ and the FCC have created a dangerous loophole: Defence rights can no longer be systematically asserted anywhere, especially when the location and manner of data collection remain secret. While the verifiability of data collection under French law was used as an argument for compliance with fair trial principles in the EncroChat case,[14] this is completely absent in the ANOM case.

While it may be true that foreign law does not need to be examined against the standards of German law, a sound assessment of *ordre public* cannot be made if the legality of an investigative measure is unclear or even not verifiable, as in ANOM. Therefore, it must be pleaded for the approach that German courts cannot completely disregard the question as to what impact unlawful conduct by foreign authorities should have on German criminal proceedings.[15] In this context, it is extremely regrettable that the FCJ and FCC adopted a highly "German-centric" approach, ignoring developments in other countries where courts are increasingly questioning the reliability of digital evidence gathered through law enforcement's infiltration of cryptophones.[16]

There were several indications that the FBI's actions were unlawful, which the German courts should have been aware

of.[17] Not to forget: There was also controversy in the United States over whether the information obtained through the infiltration of cryptophones was admissible as evidence and whether it met the requirements of the US law of evidence.[18] However, if the admissibility of the evidence is legally controversial even under US law, i.e., under the law of the originator of the action, why should other states overlook this?

2. The yardstick for an *ordre public* assessment – Did the FCJ/FCC get it right?

The courts' interpretation of *ordre public* as the ultimate limit on the admissibility of foreign evidence will be examined in this subsection. This examination will be followed by a proposal for a new approach to the issue, which shall also guide the continued analysis of the ANOM case (subsection 3 below).

Both the FCJ and the FCC derive a potential prohibition of the evidence collected abroad from scaling the *ordre public*. Both courts reduce the scope of *ordre public* to a minimum standard. In the words of the FCC:[19]

> The limits on the use of evidence [in the sense of *ordre public*] are breached if the collection of evidence abroad did not meet the indispensable minimum level of fundamental rights protection and the minimum standards under international law insofar as it binds the Federal Republic of Germany in accordance with Art. 25 of the Basic Law.

The deeper meaning of this formula is rarely clarified, and it can be debated whether such clarification is in fact possible. The decisive clue, however, can be discerned from the central norm in Germany's law on international cooperation in criminal matters: Sec. 73 IRG.[20] This provision distinguishes two types of *ordre public* in two distinct sentences:

- The rendering of mutual assistance is not permissible if it contradicts core principles of the German legal system (= national/German ordre public).
- If the request is subject to an EU instrument of judicial cooperation (e.g., the European Investigation Order), the rendering of assistance is not permissible if executing the request would go against basic principles as set out in Art. 6 TEU (= European *ordre public*).

Although the wording of the provision submits its applicability only if MLA is "rendered" (i.e. Germany as the requested state), it also applies by analogy to outgoing requests (i.e. Germany as the requesting state), as the phrasing expresses the central limit of protection of individual rights in "transnational criminal proceedings based on division of labour" (*international-arbeitsteiliges Strafverfahren*).[21] It follows that the principles underlying Sec. 73 IRG also apply to evidence collected abroad and "entering" Germany.

Against this background, the first criticism that arises is that the FCJ and FCC do not distinguish clearly enough between the national/German and European *ordre public*. The latter only applies in the realm of "EU MLA". In the ANOM case, the key questions are "who is who" and "who did what". According to the underlying facts of the case, the "third party EU Member State" did not conduct its own investigative measures, such as filtering or analysing the copied data. It merely acted as a "service" for the US authorities (FBI), as it was not permitted to place the server on US territory. "EU MLA" in the form of the EIO Directive only applies if the requested (i.e. executing) State *carries out* one or more specific investigative measures to obtain evidence (on its territory)[22]. In the present case, however, it was the FBI, as a US authority, that carried out the investigative measure, as the "final evidence product" stems from its own analysis (wherever this occured) and not from the EU. Therefore, from the perspective of the authorities in countries that received the data, the US is the "requested" State and not an EU country that merely functioned as a conduit or extended arm for the US.

As a result, only the national *ordre public* applies in the case of cooperation with non-EU Member States. This may entail higher standards than the "European *ordre public*", given that EU MLA instruments are based on a much higher level of mutual trust, which forms the basis for the concept of mutual recognition of judicial decisions. By overly emphasising the governance of mutual trust in MLA, the FCJ and FCC level this distinction and create a hurdle that is almost impossible for the individual to overcome.

In this context, a second criticism emerges: According to the courts, the *ordre public* should only come into play if the *essence* of a fundamental right – in particular the right to a fair trial (as enshrined in Art. 6 ECHR) – has been violated. It is unclear, however, why the national *ordre public* requires a further reduction of the minimum standard already set (see above) to another minimum standard, i.e., the essence of a right's violation. As *Böse* rightly stated: When evaluating evidence, German courts are fully bound by the principle of fair trial, and restricting the *ordre public* is not justifiable.[23] Similarly, the FCJ's argument that it "only" had to determine whether the proceedings as a whole were fair is flawed.[24] This approach is a consequence of the ECtHR's self-restraint, as the ECHR does not lay down rules on the administration of evidence.[25] This cannot be applied to a domestic court that must determine whether evidence, potentially obtained unlawfully (including foreign evidence), is admissible in terms of domestic law (see 1. above).

To make the assessment of *ordre public* more precise and to move away from the highly undetermined, casuistic ap-

proach of German case law, the following question should be asked: Would a tolerable situation still be guaranteed in terms of German fundamental rights and fundamental principles of its criminal procedure if the foreign standard were incorporated into German criminal procedure law for the purpose of obtaining evidence?[26]

3. Arguments in favour of an *ordre public* breach in the ANOM case

Taking this standpoint (as formulated in the previous paragraph) as the basis for the *ordre public* assessment, two arguments become apparent in the ANOM case that merit a different view to that taken by the FCJ and FCC.

a) Surveillance beyond the core values of German telecommunication surveillance law

Clandestine access to phone data through telecommunication surveillance by German law enforcement is considered a serious interference into the fundamental rights of the Basic Law (the German constitution: *Grundgesetz*).[27] To navigate this legal issue, the FCC developed several core principles that have been implemented through rather restrictive legislation in Sec. 100a et seq. StPO. In order to comply with fundamental rights, German legal requirements stipulate that surveillance orders can only be issued for serious offences that are listed and that the principle of proportionality must be observed in several respects. In addition, the German law provides for "securing mechanisms", such as requirements governing surveillance software, the permissible scope of alterations to the information technology system, their rescissions, documentation obligations, etc.[28] Notably, the FCC itself emphasised that surveillance can only be ordered on occasion of a concrete event and that the initial suspicion is concretised *ex ante* with regard to the specific list offence.[29] Indiscriminate surveillance of mobile telephones belonging to initially unknown users is therefore prohibited under German law,[30] particularly given that suspicion based on facts and events for a specific serious offence, as enshrined in the telecommunication surveillance provisions must be seen as one of the "core principles" of the German *ordre public*.[31]

The FBI's ANOM operation clearly contradicted these principles. This also cannot be discarded by the FCJ's and FCC's argument that the purchase of the ANOM crypto mobile phone *per se* establishes suspicion because "only criminals bought them". This would subject any person, criminal or not, to general suspicion of criminality and would lead to a suspicion *in rem* rather than *in personam* as is fundamentally required by German law.[32] Operating with statistical probabilities does not establish suspicion. Taken to its logical conclusion, according to the line of argumentation advanced by the FCJ and the FCC, the mere fact of holding a numbered account in the Cayman Islands would also be sufficient to give rise to suspicion of a (serious?) money laundering criminal offence.[33]

If the German BKA accepts evidence gathered in the manner of the ANOM operation, it accepts material that German law enforcement authorities would never have been permitted to collect.[34] Regardless of whether the FBI itself engaged in forum shopping or power shopping (*Befugnisshopping*), using the ANOM chats in Germany amounts to illicit power shopping on the part of the German law enforcement authorities themselves through the self-appropriation of data, which is not in line with the core principles of the German legal order.[35]

b) Disrespect for essential defence rights

Eventually, neither the FCJ nor the FCC have adequately addressed the German *ordre public* standard with regard to defence rights in digital investigations. As part of the right to a fair trial, it is common ground in Germany that the defendants and their defence council must be able to question both the lawfulness and the means and manner of enforcement of coercive measures. In digital investigations, this includes the right to have access to and voice concern over the computer data, data files established during the investigative phases, the selection process of the data by the police, their compilation, and, finally, the integrity and authenticity of the data.[36] This is consistent with the aforementioned securing mechanisms, which are framed by the German law on telecommunications surveillance as well as the procedure of digital investigations formalised in German legal practice.[37]

The FCC deemed it sufficient to be able to challenge the communication surveillance and the authenticity of the data at any time after transmission (based on reports by the BKA). However, this falls short of the fundamental principles of the German legal system, which require the *entire* "chain of custody" and data analysis to be subject to challenge.

In its existing case law on electronic evidence, and thus in determining a – potentially lower – standard of European *ordre public*, the ECtHR has also emphasised the importance of access to raw data in order to enable counter-arguments to be put forward.[38] The ECtHR likewise also emphasised the need to subject the content and integrity of the raw material to independent scrutiny.[39] Therefore, it is not

only the point in time at which evidence is used in a German criminal proceeding that is decisive, but also the point in time at which it is collected, in order to ascertain whether the essential IT forensics standards have been met.[40] By failing to disclose the circumstances of the data collection and analysis, and by refusing to provide assistance in national criminal proceedings in other states, the FBI deprives the person concerned of this essential right.[41] Ultimately, the FCC is engaging in a circular argument: If the person concerned is never provided with information regarding a chain of custody, they cannot invoke it in proceedings. This blatantly contradicts the principle of fairness.

V. Conclusion

The two rulings discussed here, by the Federal Court of Justice and the Federal Constitutional Court, have consistently upheld the approach taken in the EncroChat and SkyECC criminal proceedings, even in the – somewhat different – ANOM operation. The hotly debated question in Germany as to whether data obtained by foreign authorities through the infiltration of encrypted mobile phones using Trojans can be used in criminal proceedings with a connection to Germany has essentially been unanimously answered with a clear "yes" by both courts. The differences in the ANOM case, primarily arising from the state authorities luring offenders by distributing the mobile phones themselves via front companies, were resolved by the German courts primarily through arguments based on – almost unshakeable – mutual trust in mutual legal assistance, the virtual impossibility of reviewing the legality of foreign investigative measures, and the exclusion of prohibitions on the use of evidence under the *lex fori*. The main argument of both courts was that the limits of national and European *ordre public* were not exceeded.

The aim of this article was to demonstrate that the legal reasoning of both courts regarding mutual legal assistance could well have – and indeed should have – taken a different direction. Focusing solely on examining German rules on the use of evidence, regardless of the legality of the measure in the "requested state", falls short when it comes to the information gathering underlying the ANOM case. The courts' interpretation of the *ordre public* standard is too narrow and must be corrected by considering how the foreign rule would look like if it were incorporated into the German law of criminal procedure. Would this then give rise to contradictions with our fundamental principles? The answer to this question in the ANOM case is: Yes!

* The author would like to thank Indira Tie and Dr. Anna Pingen from the eucrim team for their careful review of the manuscript and their valuable comments.

1 BGH, Urteil vom 9.1.2025 – 1 StR 54/25. The full text (in German) is available at: <https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/Strafsenate/1_StS/2024/1_StR__54-24.pdf?__blob=publicationFile&v=1>. A press release in English is available at: <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2025_en/2025002.html;jsessionid=1EB69E7D-3CD3F4F1FD8BB40D1BEDF199.internet992?nn=19778950>. All hyperlinks in this article were last accessed on 13 March 2026.

2 BVerfG, Beschluss vom 23.9.2025 – 2 BvR 625/25. The full text (in German) is available at: <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2025/09/rk20250923_2bvr062525.html>. The English version of the decision is available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2025/09/rk20250923_2bvr062525en.html. A press release in English is available at: <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2025/bvg25-088.html?nn=68080>.

3 For the EncroChat case, see the FCJ's landmark ruling: BGH, Beschluss vom 2.3.2022 – 5 StR 457/21. The full text (in German) is available at: <https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/Strafsenate/5_StS/2021/5_StR_457-21.pdf?__blob=publicationFile&v=1>. A summary of the decision in English is provided by T. Wahl, "Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases", (2022) eucrim, 36–37. Constitutional complaints against criminal convictions following the assessment of the transmitted EncroChat data from France to Germany have remained unsuccessful (cf. BVerfG, Press Release No. 77/2023 (in German), <Bundesverfassungsgericht – Homepage – Unzulässige Verfassungsbeschwerde gegen strafrechtliche Verurteilung nach Auswertung übermittelter EncroChat-Daten>, and BVerfG, Press Release No. 104/2024 in English at: <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2024/bvg24-104.html>). On declaring evidence admissible involving SkyECC, see BGH, Beschluss vom 9.1.2025, 1 StR 142/24. The full text of the decision (in German) is available at: <https://www.bundesgerichtshof.de/SharedDocs/

Thomas Wahl
Senior Researcher, Public Law Department, Max Planck Institute for the Study of Crime, Security and Law.

Entscheidungen/DE/Strafsenate/1_StS/2024/1_StR_142-24.pdf?__blob=publicationFile&v=1>.

4 For the different approaches taken in the EncroChat case already, see J. Geneuss, "Entscheidungsanmerkung – Verwendung und Verwertung von EncroChat-Daten nach Inkrafttreten des Konsumcannabisgesetzes", (2026) *Zeitschrift für Internationale Strafrechtswissenschaft (ZfIStw)*, 104.

5 BGH, *op. cit.* (n. 1), mn. 12, 13; BVerfG, *op. cit.* (n. 2), mn. 8, 9, 31.

6 In the EncroChat case, the investigating judge in Lille, France approved a European Investigation Order; in the ANOM case, the U.S. Department of Justice approved an MLA request under the German-American Mutual Legal Assistance Treaty.

7 Cf. R. Esser, "Zur Unverwertbarkeit von Beweisen aus TK-Überwachungsmaßnahmen im Ausland („Anom")", (2025) *Wirtschaftsstrafrecht und Haftung im Unternehmen (ZWH)*, 325; L. Lafleur, "Die EncroChat-Verfahren aus Sicht der Justiz", in: K. Pfeffer (ed.), *Policing Crime Chat Networks – Lessons from the EncroChat Operation*, 2024, p. 17, 30 et seq., who justifies the use of evidence obtained in the EncroChat operation but – on the basis of the differences – sees the red line exceeded in the FBI's Anom case.

8 Act on International Mutual Assistance in Criminal Matters (*Gesetz über die Internationale Rechtshilfe in Strafsachen,* IRG). The English translation of the Act is available under: <https://www.gesetze-im-internet.de/englisch_irg/index.html>.

9 With regard to the FCJ's judgment (*op. cit.* (n.)), see M. Böse, "Anmerkung", (2025) *JuristenZeitung (JZ)*, 937; Esser, *op. cit.* (n. 7); R. Michalke, "Anmerkung", (2025) *Neue Juristische Wochenschrift (NJW)*, 1589; L. Zeyher, "Anmerkung", (2025) *Strafverteidiger (StV)*, 512; A. Althaus, "Vertrauen statt Kontrolle?", (2025) *HRRS*, 87. With regard to the FCC's decision (*op. cit.* (n. 2)): J. Marinitsch, „Anmerkung" (2025) *MMR*, 961. See also S. Pschorr and L. Wörner, "Strafverfolgung in Deutschland aufgrund US-amerikanischer Daten", (2023) *StV*, 274. At the heart of data-driven (criminal) investigations spanning multiple countries lies the more fundamental question: does the end justify the means? (cf. S. Gless, "Heiligt der Zweck die Mittel 2.0?", (2026) 144 *Schweizerische Zeitschrift für Strafrecht (ZStrR)*, 80).

10 BGH, *op.cit.* (n. 1), mn. 8; BVerfG, *op. cit.* (n. 2), mn. 27.

11 For an overview, see T. Hackner, "Vor § 68 IRG", in: Schomburg/Lagodny, *Internationale Rechtshilfe in Strafsachen*, 6th ed. 2020, mn. 11 et seq.

12 The "*forum regit actum*" principle in this sense refers to the collection of evidence (e.g., Art. 4(1) 2000 EU MLA Convention, Art. 9(4) EIO Directive) and is not to be confused with the application of the "*forum regit actum*" principle if it comes to the use of the evidence transmitted.

13 Cf. T. Wahl, "Grundlagen: Internationale Zusammenarbeit in der Telekommunikationsüberwachung", in: U. Sieber, N. von zur Mühlen, and T. Wahl, *Rechtshilfe zur Telekommunikationsüberwachung*, 2021, pp. 127 et seq.

14 BGH, Urt. v. 30.1.2025 – 5 StR 528/24, (2025) *Neue Zeitschrift für Strafrecht (NStZ)*, 371; Marinitsch, *op. cit.* (n. 9).

15 The necessity for a legality of the measure according to the law of the requested state is the prevailing approach in German legal literature. See T. Wahl. *op. cit.* (n. 13), p. 134 with further references.

16 It was revealed rather blatantly that an Australian court initially denied placing the server for the ANOM operation on Australia's territory (A. Althaus and J. Samek, "Vertrauen statt Rechtsstaat: Die ANOM-Entscheidungen des BVerfG und BGH im Lichte neuer Erkenntnisse, (2025)(6) *KriPoZ*, 396). For EncroChat and SkyECC, see S. Gless, (2026) 144 *ZStrR*, *op. cit.* (n. 9), 80; Joint Defence Team "EncroChat and SkyECC: Why European Courts are Questioning the Reliability of Digital Evidence", <https://www.joint-defense-team.com/post/encrochat-skyecc-digital-evidence-reliability-europe>.

17 C. Nestler, "Anmerkung", (2022) *StV*, 280; S. Pschorr, "Keine verfassungsrechtlich bedenklichen Erkenntnisse über die Erhebung von ANOM-Telekommunnikationsdaten?", *jurisPR-StrafR* 23/2025 Anm. 1.

18 Cf. Gless, (2026) 144 *ZStrR*, *op. cit.* (n. 9), 86; A. Milch, "'SkyECC has fallen' – Der New Yorker Paukenschlag und seine Bedeutung für Europas Kryptoverfahren", (2026) *Recht Digital (RDi)*, 46.

19 BVerfG, *op. cit.* (n. 2), mn. 29.

20 The provision is also cited by the FCJ (BGH, *op. cit.* (n. 1), mn. 19).

21 S. Gless, T. Wahl, and F. Zimmermann, "§73 IRG", in: Schomburg/Lagodny, *op. cit.* (n. 11), mn. 4; K. Ambos/A. M. Gronke, "Rechtshilfehindernisse und ordre public", in: K Ambos, S. König and P. Rackow (eds.), *Rechtshilferecht in Strafsachen*, 2nd ed. 2020, I, mn. 69. For details on the concept of the "international-arbeitsteiliges Strafverfahren", see Authors, in: Schomburg/Lagodny, *op. cit.* (n. 11), Einleitung, mn. 145 et seq. The concept reflects a shared responsibility in transnational cooperation states act collectively rather than independently. The main focus of the concept is which conclusions can be drawn for the protection of the individual who must be seen as a legal subject (*Rechtssubjekt*) in transnational criminal proceedings.

22 Art. 1(1) of Directive 2014/41/EU regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, 1.

23 Böse, *op. cit.* (n. 9), 940.

24 BGH, *op. cit.* (n. 1), mn. 36, 37.

25 ECtHR, 11 July 2017, *Moreira Ferreira v. Portugal (no. 2),* Appl. no. 19867/12, para. 83 with further references.

26 T. Wahl, "Verwertbarkeit von im Ausland überwachter Chatnachrichten im Strafverfahren", (2021) *Zeitschrift für internationale Strafrechtsdogmatik (ZIS)*, 452, 454; F. P. Schuster, *Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess*, 2006, p. 130.

27 See, recently, BVerfG, Beschluss vom 24.6.2025, 1 BvR 180/23, mn. 172.

28 See, for a summary, S. Gless and T. Wahl, "The Handling of Digital Evidence in Germany", in: M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence – Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, 2021, pp. 49, 54 et seq.

29 BVerfG, Beschluss vom 18. 4. 2007 – 2 BvR 2094/05= (2007) NJW, 2749, 2751; BVerfG, Urteil vom 27.02.2008 – 1 BvR 370, 595/07 = official case reports E 120, 274, 328 et seq.

30 LG Saarbrücken, Urteil vom 3. Juni 2024 – 4 KLs 16/24 –, juris, mn. 38; S. Pschorr, "EncroChat und (k)ein Ende?", (2025) *Strafverteidiger Forum (StraFo)*, 167, 169 with further references.

31 It is a matter of dispute whether the information gathering underlying the ANOM operation constitutes source telecommunications surveillance (as provided for in section 100a(1), second and third sentences StPO) or an online search (as provided for in section 100b StPO). See, for the distinction in general: Gless and Wahl, *op. cit.* (n. 28), p. 54. The fundamental principles are the same, however, in both provisions: an order may only be issued in respect of listed offences, the requirements of proportionality, and the need for a specific suspicion of a listed offence against a particular person.

32 R. Eschelbach, "§100a", in: H. Satzger, W. Schluckebier and R. Werner (eds.), *StPO Kommentar*, 6th. ed. 2025, mn. 21. The German courts' assumption both in the EncroChat case and ANOM case, namely that there is no case of indiscriminating mass surveillance, is opposed by the vast majority of scholars in legal literature (see, among others, Böse, *op. cit.* (n. 9), 939; Esser, *op. cit.* (n. 7), 328; Zeyher, *op. cit.* (n. 9), 514; B. Derin and T. Singelnstein, "»Encrochat« – Verwendung durch verdachtsunabhängige Massenüberwachung im Ausland erlangter Daten in deutschen Strafverfahren", (2022) *StV*, 130); F. Deutsch and T. Eggendorfer, "EncroChat – Perspektive des Rechts und der Informatik", in: Pfeffer (ed.), *op. cit.* (n. 7), p. 37.

33 Another aspect emerges in view of the essential requirements of German law: It is impossible for an ANOM-like police operation (comparable to a state-instigated "honeypot") to initially filter out individuals suspected of having committed a list offence, as required by Sec. 100a et seq. StPO.

34 Nothing else can apply if the data transfer is regarded as a chance discovery (*Zufallsfund*) or if the collection of data is seen as having been carried out for a different purpose, and the German rules of use for other purposes are applied, as done by the FCJ and FCC. Here, too, the basic requirements regarding the suspicion of a list offence and the proportionality of the original measure must be met firsthand (cf. Eschelbach, "§100e", in: Satzger et al., *op. cit.* (n. 32), mn. 20, 21; Pschorr. (2025) StraFo, *op. cit.* (n. 30), 169 with regard to Sec. 479(2), 161(3) StPO).
35 Similarly, Pschorr and Wörner, (2023) *StV*, *op. cit.* (n. 9), 281, who describe "secret service management without a mandate" ("*geheimdienstliche Geschäftsführung ohne Auftrag*"), which leads to intolerable power shopping (*nicht tolerierbares Befugnisshopping*).
36 Gless and Wahl, *op. cit.* (n. 28), pp. 68 et seq. with further references. For the crucial importance of reliability, traceability, and completeness of the right of access to files from a Swiss perspective, see Gless, (2026) 144 *ZStrR, op. cit.* (n. 9), 93 et seq. For the standard developed by the ECtHR, see J-J. Oerlemans and S. Royer, "The future of data-driven investigations in light of the SkyECC operation", (2023) 14(4) *New Journal of European Criminal Law (NJECL),* 434.
37 Gless and Wahl, *op. cit.* (n. 28), pp. 68 et seq.
38 ECtHR (GC), 26 September 2023, *Yüksel Yalçınkaya v. Türkiye*, Appl. no. 15669/20, para. 331.
39 ECtHR, *Yüksel Yalçınkaya*, *op. cit.* (n. 38), para. 332.
40 F. Meyer, "Übermittlungsvoraussetzungen und Verwertbarkeit von EncroChat-Daten, (2024) *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)*, 243, 250, 251. For the "ECHR standard", see also R. Stoykova, "Encrochat: The hacker with a warrant and fair trials?", (2023) 46 *Forensic Science International* 301602.
41 For a similar result, see Böse, *op. cit.* (n. 9), 940, also referring to ECJ, 30 April 2024, Case C-670/22, *M.N. {EncroChat]*, paras. 105, 130; Esser, *op. cit.* (n. 7), 329.

How to Design a Surveillance Barometer

Model for the Regular Monitoring and Assessment of Statutory Powers and Practices in State Surveillance

Michael Kilchling and Sabrina Ellebrecht*

Surveillance by government agencies profoundly impacts daily life and raises fundamental questions for Germany's liberal constitutional order. Yet, public debate on surveillance powers often lack insight into actual surveillance practices: Which measures are used, how often are they used, and under what conditions? As the frequency of surveillance increases, the real and perceived risk of being monitored by the police, prosecutors, or security agencies also rises. To address this gap, the Max Planck Institute for the Study of Crime, Security and Law (MPI-CSL) in Freiburg has developed a pioneering surveillance barometer — a tool for the systematic, evidence-based assessment of surveillance measures in Germany. A prototype for a dynamic online platform is currently under development. It will enable transparent monitoring, support evidence-based policymaking, and serve as a model for similar initiatives across the EU. Ultimately, the Surveillance Barometer aims to foster informed debate, reduce concerns regarding a possible erosion of fundamental rights, and strengthen accountability in the implementation of security policy. In the longer term, it could help avoid misconceptions in the public discourse by ensuring the debate is grounded in factual data. This transparency is essential for building trust and ensuring that any form of surveillance remains both effective and constitutionally sound.

I. Introduction

The production, retention, seizure, and processing of a variety of sensitive data about citizens and their activities in everyday life,[1] together with other forms of surveillance carried out by state agencies, have been at the centre of democratic discourse – in politics, juristic and other academic circles, NGOs, the media, and civil society – for decades. Driven by the steady expansion of such powers – technically facilitated by digitalisation, and politically propelled by EU legislative demands – some critical observers have even predicted nothing short of the end of privacy.[2] One of the key turning points in this development was the introduction of the groundless temporary retention of telecommunications metadata from all citizens, stored as a standard resource at the disposal of prosecution agencies. Notwithstanding the erstwhile lack of legislation powers in penal matters[3] the instrument was pushed by the European Union (EU), regardless of opposing positions in some of the Member States and the established case law of their constitutional courts. Even after the nullification of the original directive[4] by the European Court of Justice,[5] *data retention*

has remained on the agenda in most Member States and continues to be one of the most powerful trigger words in the critical security policy discourse.[6] It has become a metaphor of today's "surveillance society,"[7] a phenomenon that is particularly evident in the German context.[8]

II. Assessment of the Impact of Surveillance from a Supra-individual Perspective

Academic discussion about surveillance and its constitutional limits in Germany was largely stimulated by the Federal Constitutional Court's (FCC, *Bundesverfassungsgericht – BVerfG*) 2010 landmark ruling on the limits of telecommunications metadata retention under constitutional law.[9] As one of its key arguments, the Court held that excessive precautionary surveillance of citizens would be incompatible with the constitutional identity of the Federal Republic of Germany, which implies that the state must not record and register citizens' exercise of their freedoms in its entirety. In a side note, the judges in Karlsruhe further held:

> "[W]ith the precautionary retention of telecommunications traffic data in place, there is considerably less leeway for allowing other types of data gathering not based on specific grounds, including for measures originating at EU level."[10]

The FCC had further emphasised that these constitutional principles require *"greater restraint by the legislature"* when considering introducing additional data retention powers.[11]

1. Need for an impact assessment

In scholarship, *Alexander Roßnagel* developed and promoted the idea of the need for a comprehensive review of all existing surveillance powers, called *"Überwachungsgesamtrechnung"* [general surveillance calculus].[12] In the following years, this topos – which appears both catchy and cumbersome – was picked up in legal, political, and societal discussions and referred to as key argument in favour of establishing a critical record of all existing surveillance powers provided to state agencies. The discussions addressed not only the law enforcement sector but also other areas of (interventionist) public administration, including preventive policing, customs and finance, transportation, digital services, and not least the intelligence sector. This broad approach is based on an additive understanding of the impact that the mere existence of the various statutory surveillance powers and their potential use has on the potential infringement of fundamental freedoms.[13]

Contrary to what the term "general surveillance calculus" actually implies, the approach has mainly been discussed theoretically (on a qualitative, doctrinal level) and less from a practical perspective (in that it was only rudimentarily operationalised). By focusing on surveillance powers from an abstract point of view, previous analysis has failed to address whether and to what extent surveillance practices are in fact applied. In this regard, we are still groping in the dark. We are currently unable to quantify whether the "burden of surveillance" in the country has actually changed over the past decade(s), nor can we determine its overall scope. The associated infringement of fundamental rights materialises only when the available legal powers are in fact exercised by the state. Therefore, the key question regarding the – constitutionally acceptable – level of state surveillance is also a quantitative one. This is because, as the frequency of such measures increases, so does the statistical probability of being targeted individually.

The quantity issue, however, is often neglected in critical discussions on surveillance. While the individual risk of actually becoming being targeted by a covert remote computer search ("online search" – *Onlinedurchsuchung*) is virtually close to zero, due to the small number of cases in which it is used,[14] the constant monitoring of financial data affects almost all citizens. From both a qualitative and a quantitative perspective, the mass surveillance of financial data — not least because of its promotion and continuous expansion through EU legislation[15] — is likely one of the most extreme examples of indiscriminate and ubiquitous data retention.[16] This is even more the case than with flight passenger data recording, which has been considered an extreme example of excessive data retention in recent years.[17] Whereas passenger flights are a relatively rare activity in the daily life of the average citizen, financial transactions are carried out regularly and, with the growth of cashless payments, often several times a day. This can be considered a prime example of an excessive precautionary surveillance of citizens, as problematised by the FCC in its 2010 ruling. Surprisingly, this dimension of surveillance has not yet received much public attention, presumably also due to a lack of information.[18]

Indeed, it seems imperative not only to look at surveillance and its impact through a doctrinal lens, but also to incorporate empirical reality into the assessment. The fact that this has not been done in the past can be explained, at least in part, by the fact that reliable statistical information on the frequency of surveillance measures, especially when carried out in a preventive context, has long been only sporadically available or even unavailable. This is a crucial gap that must be gradually closed in the coming years.

The Freiburg Max Planck Institute for the Study of Crime, Security and Law (MPI-CSL) has developed and pre-tested the model and methodology for establishing a Periodic Surveil-

lance Barometer (*Periodisches Überwachungsbarometer*). It combines two perspectives: an assessment of the normative shape of the various surveillance powers in force (legal perspective) and their application in practice (empirical perspective). This conceptual approach enables the systematic evaluation of the *burden of surveillance* to which citizens are subjected in a specific reference period (e.g., calendar year), based on a standardised set of qualitative and quantitative variables. "Burden" refers to the general risk of being targeted by a surveillance measure, as well as the impact of surveillance practices on the actual level of protection of fundamental rights in society as a whole. From a doctrinal perspective, this touches upon an additional aspect of the nature of fundamental rights, one that more recent contributions have addressed as the objective dimension of fundamental rights[19] protection.[20] *Marcus Löffelmann* published proposals for a concept similar to the MPI-CSL's Surveillance Barometer, which not only seeks to quantify the societal costs of security-related surveillance measures but also takes into account their potential societal benefits.[21]

2. Traditional assessment models

Concepts for assessing the concrete degree of (potential) infringements on individual rights have been discussed in surveillance studies[22] from a variety of theoretical and practical perspectives. These include models and proposals for, e.g., impact assessments of human rights violations,[23] privacy impact assessments,[24] data protection impact assessments,[25] and surveillance impact assessments,[26] the latter sometimes with a particular focus on the economic costs of surveillance.[27] Adopting an even broader perspective, *Wright* and *Raab* point to potential social, economic, financial, political, ethical and psychological impacts of surveillance.[28] In some jurisdictions, different types of impact assessments are already in place, also as a standard element in the drafting processes for legislative acts; quite often, however, they are criticised for their lack of any solid empirical background.[29] All such models share, however, a significant shift from an individualist perspective to a systemic risk perspective — one that moves from an *ex post* assessment of individual harm to the evaluation of potential fundamental rights risks for citizens and society as a whole.[30]

Of particular importance is the assessment of the intensity of infringements of fundamental rights. Independent of the concrete terminology referred to – seriousness, severity, gravity, magnitude, etc.[31] – intensity has always been a key parameter of the proportionality test in many legal systems.[32] Following this tradition, the FCC's case law provides an extensive casuistry of categories, ranging from "minor *[gering]*" or "slight *[geringfügig]*" at one end of an imaginary scale to "very intrusive *[tiefgreifend]*" or "particularly serious *[besonders stark]*" at the other end; infringements of a medium degree have been characterised as, e.g., "of considerable weight *[von erheblichem Gewicht]*" or just „weighty *[gewichtig]*."[33] This qualitative assessment technique conveys a certain quasi-empirical appearance. In its very essence, however, it is of an intuitive nature. This carries with it a certain risk of imbalance and uncertainty, which can sometimes even be detected in actual court decisions.

Interestingly, the FCC's 2010 ruling on telecommunications metadata retention itself provides proof of this problem: in the two dissenting opinions, considerable contention about the extent to which data retention practices may interfere with citizens' fundamental rights has been documented. While the majority vote considered the interference to be "particularly serious," the first dissenting judge characterised it as less serious; instead of "particularly serious," his final rating was "particularly weighty."[34] Similar considerations were put forth in the second dissenting opinion, which concluded that "[obviously – *sic!*] the weight of interference [… induced by telecommunication metadata retention …] is *minor* and cannot be compared to the weight of interference resulting from access to communication contents."[35] The disparity between the majority's opinion and the second dissenting opinion could not be more profound, given that "particularly serious" denotes the most severe type of interference conceivable according to the FCC's current scale.[36]

The dissenting opinions reveal a principal shortcoming of the concept as currently applied. What might appear to be an issue of semantics is the result of a lack of consistent and evaluable criteria. What specifically makes the difference between, e.g., an infringement of a "considerable *[erheblich]*" extent and one of a "not inconsiderable *[nicht unerheblich]*" extent, and what is the threshold between them?[37] Instead of a descriptive scaling, developed and continually refined on the basis of emerging case law – which is as selective as it is arbitrary[38] – a more generalised concept based on definite and measurable parameters should be applied.

3. Empirically grounded assessment

As outlined above, a purely normative assessment method is insufficient for capturing the impact of surveillance. What is needed is a theoretically and empirically sound operationalisation of the impact assessment that reveals the true level of surveillance that citizens are exposed to in their daily lives as a result of the *actual* use of various statutory

powers by the authorities. Unlike traditional proportionality doctrine, the Surveillance Barometer is not concerned with the abstract (constitutional) legality or illegality of a measure, but with its concrete impact on those affected, considering not only the individual but also the collective of fundamental rights holders.[39] From this perspective, *any single intervention* constitutes a relevant infringement, including all proportionate and lawful measures. Taken together, these measures minimise the areas in which constitutionally protected freedoms can be exercised – that is (in our context), surveillance-free spaces. This explains why the frequency with which individual surveillance measures are applied is an essential factor in assessing the extent of state surveillance.[40] In its case law, the FCC has traditionally considered prevalence indirectly at most, for example by requiring highly protective statutory restrictions for serious infringements, thereby aiming to curb excessive surveillance. However, concrete figures have not yet been taken into account.

Unlike earlier proposals,[41] the MPI-CSL's Surveillance Barometer systematically includes empirical aspects. The concept applies to the two main elements of its intensity assessment method:

- A determination of the seriousness of the basic rights infringements by means of uniform and measurable criteria;
- A systematic account and classification of how frequently the various surveillance powers are being applied.

Taken together, the concept is both theoretically and empirically sound: all potential surveillance scenarios can be accurately measured and put into relation with each other. This makes it possible, for the first time, to identify trends and draw a wide range of comparisons between specific types of surveillance measures, agency sectors, regional practices, and time periods. As a result, several questions can be addressed, e.g.:

- Has the number of surveillance activities and/or their intensity increased in recent years due to the introduction of new legislation or changes in application practices?
- Has the level of surveillance ever decreased, e.g., in the wake of a crisis such as the COVID-19 pandemic?
- Are fundamental rights holders in federal state A possibly subject to greater surveillance than those in federal state B, because the police in A increasingly resort to telecommunications metadata or digital services, while those in B prefer traditional search and seizure?

In the following section, we will present the methodological concept of the MPI-CSL's Surveillance Barometer, together with some preliminary findings.

III. Six-Step Methodology

1. Identification of surveillance powers

The first step is to identify the relevant surveillance scenarios to be covered by the Surveillance Barometer. These include both the targeted production of data about individuals by state agencies through physical methods (e.g., covert observation) or technical methods (e.g., telephone tapping), as well as the retrieval of data generated and owned by third parties (service providers or the private individuals themselves). The latter is mainly carried out through production orders that concern existing data, realtime data, and data that will be generated in a future period of time. From the perspective of the basic rights holders, the most appropriate approach emerged as a systematisation according to sensitive spheres of private life where extensive personal data is continuously generated – knowingly and unknowingly – which could potentially be tapped via the various types and methods of surveillance. *Figure 1* illustrates the sensitive spheres of daily life in which citizens are particularly vulnerable as regards infringements of their privacy.

Above all, one's private home is of explicit sensitivity in this regard, as it is at the core of one's private life. Audio and video surveillance of private premises are only two of many methods of covert surveillance. In addition, any physical objects and data repositories including computers, electronic devices, and smart home gadgets can become targets of standard search and seizure operations in this private sphere. Besides the immediate seizure of portable home devices, data can also be gathered remotely from commercial service providers. Alongside the private home, communication, the usage of social media and other online activities are accordingly relevant spheres as they generate numerous types of digital traces, including inventory data, traffic data or metadata, passwords, activity data, and not least the very contents of the communications, whether oral or written. Similar vulnerabilities exist in relation to people's finances. This goes far beyond the traditional registration of property and income ownership. The globalisation and digitalisation of financial services, together with the trend towards cashless payments, have paved the way for a fundamental expansion and intensification of surveillance powers, enabling a greater number of agencies to gather and distill detailed insight into how individual citizens conduct their lives. Lastly, people's presence in public has traditionally provided many opportunities for exposure to observation. Today, mobility has become a target point for a variety of new surveillance powers. In addition to the afore-mentioned record of PNR data (see above, II.1.), automobility is a key producer of sensitive data: personal data

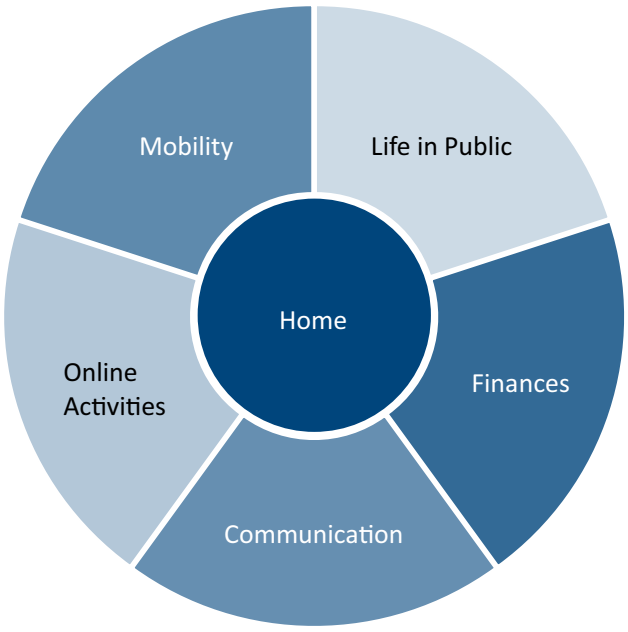

Figure 1: Sensitive spheres of private life subject to surveillance

about car owners and their driving behaviour, technical data automatically generated by the car itself, data recorded by the manufacturer, etc. These data can be generated by state agents through speed control, digital parking control, automated section control based on automated licence plate recognition, GPS tracking, etc. or through the seizure of existing data, e.g., records from the navigation systems, technical information, data generated by connectivity services, dashcam content, and, most controversially, image and video records from Tesla's Sentry Mode.

2. Normative analysis of regulations

Based on this analytical structure along the five most sensitive spheres of private life, the MPI-CSL's research team collated a full record of all relevant legal provisions under which police, prosecution, customs and intelligence agencies[42] are permitted to collect data or other forms of personal information.[43] In total, the research team identified some *3,500 statutory provisions and sub-provisions*[44] under which the competent security agencies in Germany are permitted to initiate surveillance operations.[45] Such provisions quite often include several statutory alternatives of the same type of measure to which diverging legal and/or situational conditions apply. These conditions include specified catalogue crimes, different degrees of suspicion, and different threat categories, etc. The measures must be organised and operated in different ways – for example, differing in scope or threshold, or governed by either more lenient or more restrictive procedural rules. As a first key product, the Surveillance Barometer enables comprehensive surveillance maps to be designed. These maps offer people the opportunity to trace the different areas in which they are effectively at risk of being subject to an infringement of their privacy. It also allows them to retrieve detailed information about which agency can tap into which sphere of life, according to which regulation, and under which rules. In the near future, dynamic surveillance maps will be made accessible to the general public in an online database.[46]

3. Normative intensity assessment

Another core element of the MPI-CSL's further analyses is the assessment of the normative intensity of the fundamental rights infringements that go with state surveillance, based on a set of standardised criteria. To this end, a complex category system was developed that takes into account all characteristics that can be assigned in an abstract manner and quantifies them according to their relative constitutional weight. From the voluminous body of the FCC's case law, a total of 18 abstract parameters[47] were extracted in order to assess normative intensity in detail. Functionally, two types of criteria must be distinguished.

The first group consists of factors which constitute the basic severity of infringement. These include the privacy grade of information acquired, the aim and duration of an operation, and the potential impact on third parties (see *Table 1a*). Next to these constituting factors, the second group comprises potential mitigating circumstances. These features, which aim to alleviate the potential impact of fundamental rights infringements, are an essential part of security legislation in the form of, e.g., regulations on legal and operational thresholds, procedural safeguards, and mechanisms of internal or external control, either *ex ante* or *ex post* (see *Table 1b*). Both groups of factors consist of nine variables, each subdivided into several sub-categories (items) and rated on a scale from 1 and to 10. However, the various factors do not all carry the same constitutional weight. These differences have been taken into account by assigning individual weighting factors, which also range between 1 and 10 (see *Tables 1a and 1b* again). The values of the constituting and the mitigating factors have been inversely scaled according to their distinct function. Altogether, intensity can be determined according to 118 items.[48]

The next step is to calculate the refined normative intensity scores, which are composed of the respective severity and mitigation scores of each statutory variant. Rather than simply multiplying the two scores, a mitigation formula[49] was developed to reflect the relative weight of the mitigating factors. This implies that statutory safeguards cannot

Constituting Factors			
	Criteria	Weighting factor	Relative weight (%)
1.	Privacy grade of information acquired	10	32
2.	Spread width (potential impact on third parties)	4	13
3.	Recourse on retained data	4	13
4.	Maximum duration	3	9.5
5.	Temporal direction	3	9.5
6.	Degree of covertness	3	9.5
7.	Role of person(s) targeted	2	6.5
8.	Method/technique used	1	3
9.	Aim of surveillance measure	1	3
	Total	**31**	**99**

Table 1a: Factors constituting basic severity

Mitigating Factors			
	Criteria	Weighting factor	Relative weight (%)
1.	Legal threshold: protected legal interest/reference crime	10	25
2.	Operational threshold: type of (potential) threat/degree of suspicion	10	25
3.	Requirements for authorisation	5	12.5
4.	Additional formal safeguards	5	12.5
5.	Protection of those entitled to refuse to testify	3	7.5
6.	Duty to erase collected data after use	3	7.5
7.	Duty to notify those affected	2	5
8.	Duty to keep track records	1	2.5
9.	External control mechanism	1	2.5
	Total	**40**	**100**

Table 1b: Mitigating factors

	Severity score (S)	Mitigation score (M)	Refined normative intensity score (NI)
Minimum	3.348	1.343	3.055
Maximum	8.0	8.143	7.342
Mean	5.756	5.111	5.312
Median	6.0	5.175	5.448

Table 2: Key scores of all relevant provisions under review (Germany, 2022)

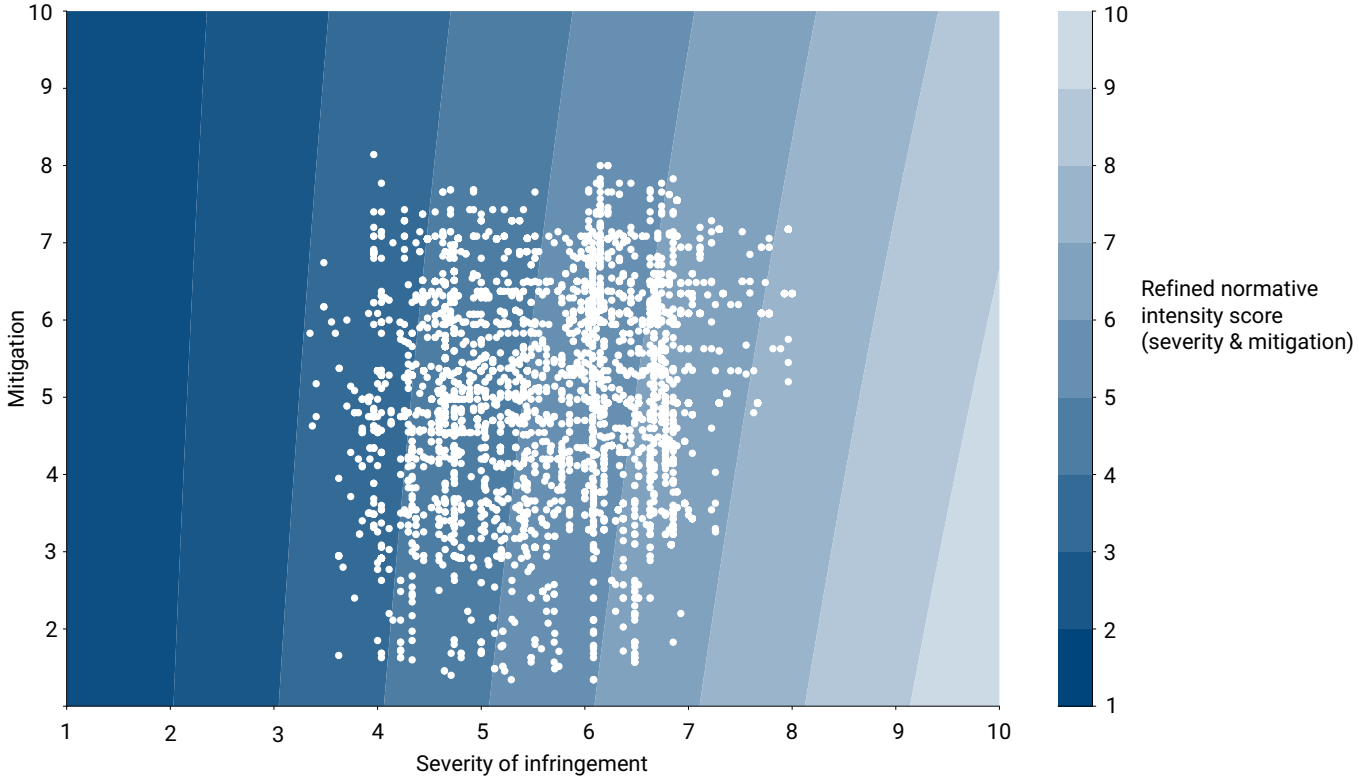

Figure 2: Refined normative intensity scores (Germany, 2022)* / Contour Plot for NI = S – S (0.15 * M / 10) and NI >=1.

counterbalance the true impact of a fundamental rights infringement, neither to a major nor even to a full extent. Otherwise, it might so happen that a measure of high severity, which regularly goes hand in hand with high protection standards (e.g., a covert remote search of a private computer), and a measure of low severity, to which no or only minor procedural constraints apply (e.g., an automated inventory data request), score similarly. As a result of intensive preliminary testing, the maximum possible reduction effect of mitigation was set at 15 per cent of the severity score, decreasing with lower severity.[50]

Having completed the normative intensity assessment for all the relevant statutory provisions and their variants in force in 2022,[51] the research team's findings provide detailed insight into the intensities of the fundamental rights infringements. *Table 2* provides an overview of the variance in the three normative scores. While the basic severity of statutory surveillance powers varies between 3.348 and 8.0, refined intensity scores that take into consideration the mitigating factors are moderately lower, ranging between 3.055 and 7.342. The variance is significantly broader when looking at the configuration of the statutory safeguards, as reflected in the mitigation score. The minimum is 1.343 and the maximum is 8.143. This indicates, firstly, that there is a broad range of legislative options for achieving a (more) protective configuration of surveillance powers, and, secondly, that legislatures do in fact make use of such moderating techniques in different ways and to varying degrees. It follows that the same powers are often regulated in different ways in the respective laws, with mitigation scores varying by more than 30 per cent.[52] These findings underline the fact that legislatures in fact have considerable – political – leeway in shaping surveillance powers and, in doing so, determine the concrete levels of basic rights protection.

Overall, intensities score above average. This is also confirmed by the fact that the median intensity is higher than the corresponding arithmetic mean. *Figure 2* illustrates the three-dimensional dispersion of the scores for all variants. It provides interesting insights into the general shape of surveillance powers in Germany. The pattern depicts a phenomenon that has been theoretically discussed in the literature as the unitising effect of the Federal Constitutional Court's rulings on the general standards of statutory basic rights protection. This supports the premise that key rulings by the FCC on a particular aspect of a single piece of legislation shape the margin of legislative autonomy to the effect that relevant laws tend to approximate, in particular, new or amending laws on the same subject matter that are subsequently passed.[53] In addition, extreme statutory configurations are prevented; there are no outliers at the far end of the scale. Across all provisions, however, the variance in mitigation (y-axis) is considerably high for most

of the severity grades identified. The protective regulations governing surveillance powers scoring at around grade 4, for example, are as diverse as those for most of the powers scoring at grade 6 or even 6.9. Consequently, surveillance powers of the same severity grade that come with very high protection standards (between grades 7 or 8) in one case may be mitigated to a significantly lower degree in another, sometimes even lower than grade 2. This implies that the various legislatures pursue different policy priorities, which are realised through their distinct employment of mitigating factors. Only surveillance powers at the highest severity levels (i.e., higher than grade 7 on the x-axis) are subject to significantly high(er) protection standards such as, e.g., strict judicial ex ante control.

As illustrated, the normative data provided by the Barometer reflects the potential and limits for the statutory regulation of surveillance in Germany. The scores describe the normative level of surveillance in terms of the assessment of existing surveillance powers. The frequency with which these powers are used is not yet included in this analytic step.

4. Quantitative dimension of surveillance

In addition to the normative intensity of the relevant basic rights infringements, their frequency is of equal importance when assessing the general level of surveillance in a society. The reason for this is because the statutory potentialities identified and evaluated in the previous step only materialise via their operational implementation (see also above, II.3.). It should also be borne in mind that the greater the number of surveillance operations carried out, the more vulnerable a society becomes as a whole. This is why the number of surveillance measures conducted is an additional element of the Surveillance Barometer concept. In a subsequent work package, the relevant statistical data must be collected for each surveillance provision identified. These data will be aggregated into frequency scores that carry equal weight in the final formula. In addition to the absolute frequency the density, i.e. the relative frequency in relation to the resident population, is taken into account.

Methodologically, two challenges need to be solved. First, the calculation model must balance out extreme quantitative imbalances that arise between surveillance measures that are extremely rare (such as dragnet investigations or remote computer searches with no more than a handful of cases per year) and cases of mass surveillance involving hundreds of thousands or even millions of applications per year (such as banking data queries or automated retrievals of telecommunications inventory data). To keep quantifications manageable, absolute numbers will be converted into indexed frequency coefficients with values between 1 and 10. Assuming that low numbers are much more prevalent than high ones, and that rare applications correlate with high and very high intensity, indexing will be carried out on the basis of a logarithmic scale to allow for a more detailed count in the lower intervals.[54]

Secondly, imbalances arising from differences in citizens' actual exposure to surveillance, caused by the fragmentation of legislative and operational competences in the Federal Republic of Germany, need to be taken into account. For example, there are the surveillance measures imposed by federal agencies acting under federal law, e.g., involving the Federal Criminal Police Office of Germany (BKA). These federal measures have a different overall impact than those carried out under state laws, which only capture subjects under the respective state jurisdictions. Consequently, calculations must also reflect differences in the regional populations. One way to address this impact disparity, is to aggregate frequency as incidence rates per 100,000 inhabitants – a well-accepted standard epidemiological method established in other areas of security policy, e.g., to portray crime rates and incarceration rates. At the same time, incidence rates can serve as an easily comprehensible reference frame for the general public, a concept which also gained popularity during the COVID-19 pandemic.

5. Surveillance scores

Both parameters – the intensity and the frequency of all the different surveillance measures – are the core elements of the MPI-CSL's Surveillance Barometer. Representing the *normative (constitutional) intensity and empirical frequency* of interventions, these elements must be combined in the fifth step. The respective surveillance scores can be generated by multiplying the intensity and the incidence scores, each ranging from 1 to 10. These scores then vary between 1 and 100 on a closed scale. This step is only possible if data on the frequency of the various surveillance measures is available. Ideally, in the future, surveillance scores should be provided for all surveillance measures effectively carried out in a calendar year – categorised by the specific statutory surveillance powers under which they are authorised. Currently, most agencies in Germany are not yet prepared to produce and deliver the necessary data for various reasons (see below, IV.).

6. General surveillance indices

The final step of the concept is the aggregation of the various scores into general surveillance indices to provide a comprehensive overview of the state of surveillance in the

country and the relevant areas in which citizens' right to privacy is more or less vulnerable to state surveillance activities. These indices can be aggregated according to several parameters distinguishing between national and regional levels, between different sectors (e.g., policing, prosecution, and intelligence), and between the types and techniques of surveillance (e.g., telephone tapping, acoustic surveillance of private premises, retrieval of financial data, remote computer searches, and GPS tracking[55]).

At the moment, the Surveillance Barometer is fully operational for the delivery of normative intensity values only. *Figure 3a* shows the averaged normative indices for German surveillance powers under federal law and under state law. It shows that the general level of surveillance intensity associated with the respective statutory powers is lowest in the state of Saxony and highest in Saarland. The average intensity of federal powers is also moderate, with an overall score that remains below the average of all of them.

The overall picture, however, changes significantly when viewing the accumulated impact (*Figure 3b*). When all surveillance powers are added up, the total number of statutory powers under federal law far exceeds that of the federal states, by more than 100 per cent. This is due to the existence of specialised federal agencies that have no state-level counterparts[56] and the sheer multitude of their powers, some of which are even exclusive, such as the collection and analysis of PNR data by the BKA. Their number alone also contributes to the level of surveillance, as it naturally increases the likelihood of individuals being targeted by a federal agency rather than a state agency.

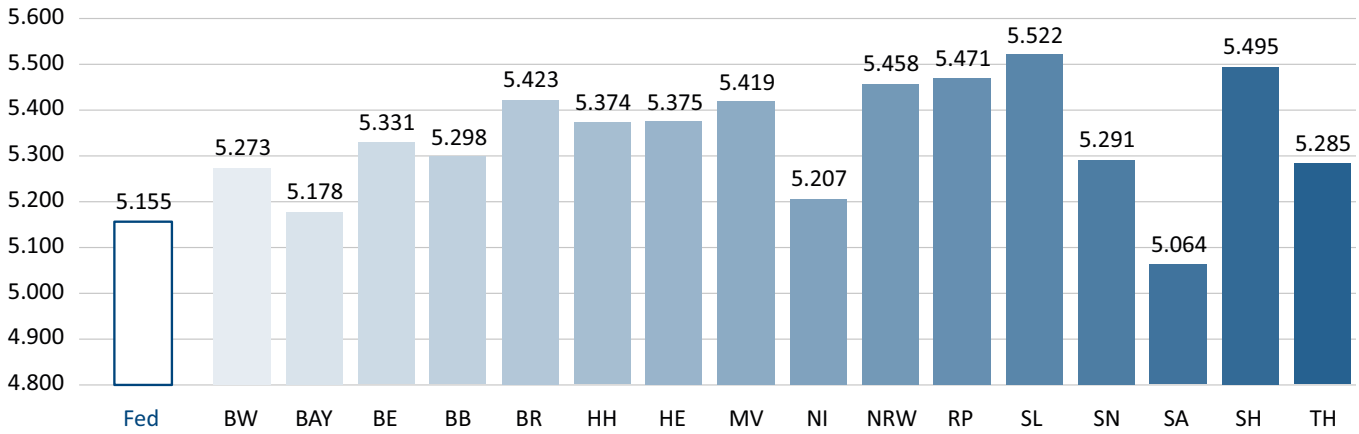

Figure 3a: Normative surveillance scores – averaged: Federal level and federal states (Germany, 2022)*

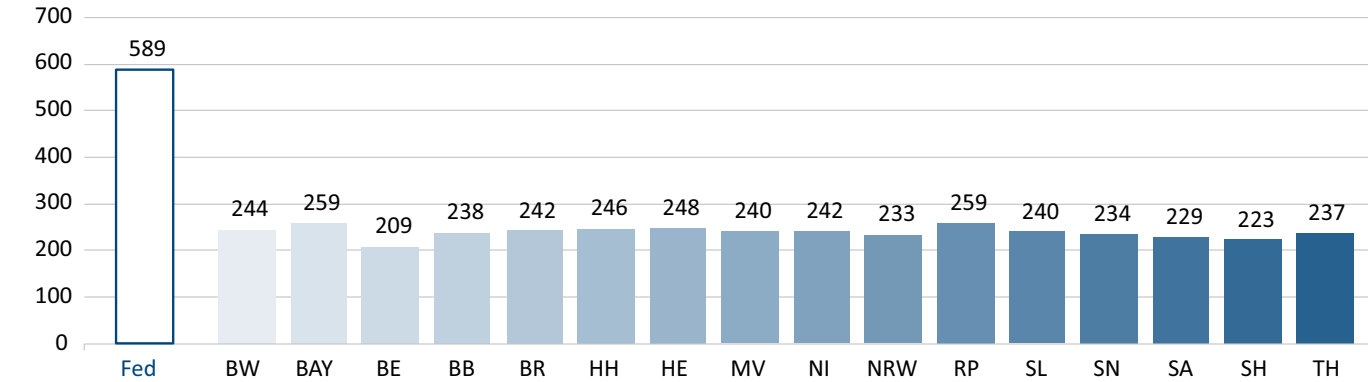

Figure 3b: Normative surveillance scores – accumulated: Federal level and federal states (Germany, 2022)*

* Fed. = Germany Federation, BWE = Baden-Württemberg, BAY = Bavaria, BE = Berlin, BB = Brandenburg, BR = Bremen, HH = Hamburg, HE = Hesse, MV = Mecklenburg-Western Pomerania, NI = Lower Saxony, NRW = North Rhine-Westfalia, RP = Rhineland-Palatinate, SL = Saarland, SN = Saxony, SA = Saxony-Anhalt, SH = Schleswig-Holstein, TH = Thuringia.

The category system, with its detailed set of variables, enables all types of surveillance to be compared with one another. Presenting the data in the form of specified indices reveals both the total, cumulative burden of surveillance and its composition. In particular, this enables key areas of surveillance and potential critical levels of surveillance within individual sectors to be identified and pinpointed. The model is not static but can be flexibly adapted to the current legal status quo within the relevant reference period. This makes it well suited for responding to rapid regulatory developments, which are characteristic of security law.

IV. Outlook

The MPI-CSL's Surveillance Barometer is a valuable instrument for mapping and measuring both the extent and impact of surveillance actions on individuals and the resident population. Moreover, it highlights the potential for enhancing fundamental rights protection through the systematic identification of opportunities for regulatory adjustment. This is the first time that a thorough assessment model based on a uniform set of criteria has been tested in the field of state surveillance. Once established as a scientifically based transparency project for Germany, it can easily be modified and adapted for application in other jurisdictions.

However, the path towards reinforcing transparency in the use of surveillance powers is not merely a matter of political expediency; it also has a clear constitutional dimension. In the FCC's case law, transparency in the operations of public agencies has gained increasing importance as a fundamental prerequisite for proportionality. Among other things, the Court established a constitutionally grounded duty to implement effective record-keeping practices for all measures involving a fundamental rights infringement.[57] In the context of government surveillance measures, in particular, transparency has two dimensions: (1) an individual dimension focusing on those directly affected, and (2) a societal dimension. Regarding the latter, further internal and external aspects can be distinguished. These include the function of transparency as a prerequisite for effective professional oversight and judicial control, for democratic control in the political arena and society, and for internal organisational control and resource management.[58] In Germany, the most urgent practical challenge to date is to remedy the lack of reliable statistical data on the application of statutory powers, including surveillance operations. This sparse availability of data leaves the public in the dark about their use. In this regard, the grim picture of a surveillance society – often expressed by human rights activists[59] – could be seen as a *symptom of a lack of transparency*.

In Germany, the unavailability of data is also the result of structural deficits in digitalisation. It is not uncommon still for annual counting lists to be compiled by manually browsing paper files. At the same time, digital case management systems used in the police force and in other public sectors have been configured to disable automated record functions deliberately, in order to prevent unlawful performance monitoring and to dispel eventual data protection concerns.

Yet, a promising policy tool, which has received increasing attention in recent years as an instrument to generate better availability of statistical data, involves statutory duties to produce and publish statistical records about the use of specific measures considered to have the potential to seriously infringe fundamental rights. Telecommunications surveillance and remote online searches of private computers are exemplary areas in which the FCC's calls for greater transparency have led to the introduction of transparency provisions. Such regulations can currently be found in the German Code of Criminal Procedure,[60] the Federal Criminal Police Office Act,[61] and many state police laws,[62] for example. In most cases, however, these provisions cover only a very limited number of surveillance powers, primarily those that have been the subject of public controversy and political resistance in parliamentary proceedings. They have also been used as an incentive to get the relevant bills passed. These provisions differ significantly from one another in terms of both form and content. So far, the statistics have sometimes only been provided to the respective parliamentary bodies and are not always publicly accessible. In direct comparison, Sec. 101b of the Code of Criminal Procedure[63] appears to be the current gold standard as the Federal Office of Justice (*Bundesamt für Justiz*) publishes the data online.[64] With an advanced judicial and political pressure, the volume of data provided by other agencies should also increase in the coming years. Subsequently, these statistics will become an important resource for the Barometer.

Ultimately, the Surveillance Barometer concept could be used as a blueprint for developing a Europe-wide transparency monitor.[65] From an EU perspective, it could be applied as an analytical tool to help the European Commission and/or the European Parliament and its committees conduct comparative evaluations of how EU laws have been implemented in national legislation across Member States. Experience gained from the German pilot project could be a useful incentive for this purpose. At the European level as well, the availability of necessary statistical materials is expected to improve steadily, as EU legislation increasingly mandates statistical data collection from Member States. The requirements for the quality and validity of data provided have been enhanced over time. Whereas older acts such

as, for example, the 2012 Victims' Rights Directive[66] or the 2013 Cybercrime Directive[67] oblige Member States only to provide "data and statistics" (in the latter example only in three-year cycles), more recent pieces such the 2024 Asset Recovery and Confiscation Directive[68] have been setting forth significantly higher standards, requiring the production and maintenance of comprehensive statistics on a variety of concretely specified types of data,[69] to be delivered on an annual basis. Even more extensive are the requirements for the statistical recording of more or less all relevant activities carried out in the field of money laundering control.[70] Consideration should also be given at EU level to establishing a more systematic framework for the provision of meaningful statistic records. In the end, European statistical requirements may have a positive impact, as they can also help increase the availability of national data, which did not previously exist or were not publicly accessible at the domestic level.

* The authors would like to thank Indira Tie, Dr. Anna Pingen, and Thomas Wahl from the eucrim team for their careful review of the manuscript and their valuable comments.

1 This includes both data owned by citizens and data generated and administered by public agencies or commercial service providers.

2 P. Schaar, *Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft*, 2007.

3 In absence of an explicit competence in pre-Lisbon times, the initiative was inappropriately promoted as a subject of market regulation. Cf., e.g., H.-J. Albrecht, A. Grafe & M. Kilchling, *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h der Strafprozessordnung*, BT-Drucksache 16/8434 of 28.02.2008, pp. 41 et seq., <https://dserver.bundestag.de/btd/16/084/1608434.pdf>; A. Adensamer, *Handbuch Überwachung*, 2020, pp. 34 et seq. Note: All hyperlinks in this article were last accessed on 28 April 2026.

4 Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, OJ L 105, 13.4.2006, 54.

5 ECJ, 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland, Seitlinger & Others*, EU:C:2014:238.

6 Cf., e.g., Fennelly's notion of the "life, death and afterlife" of that directive: D. Fennelly, "Data retention: The life, death and afterlife of a directive", (2019) 19(4), *ERA-Forum*, 673–692. For the debate on data retention at the EU level, see also T. Wahl, "Council: The Way Forward in Data Retention", (2019) *eucrim*, 106 with further news references; A. Juszczak and E. Sason, "Recalibrating Data Retention in the EU", (2021) *eucrim*, 238–266.

7 Cf., e.g., R. Sarre, "The Surveillance Society: A Criminological Perspective", in: E.C. Viano (ed.), *Cybercrime, Organized Crime, and Societal Responses*, 1985, pp. 291–300.

8 Cf., e.g., P. Schaar, *op. cit.* (n. 2); T. Singelnstein & P. Stolle, *Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert*, 2008; N. Zurawski (ed.), *Surveillance Studies. Perspektiven eines Forschungsfeldes*, 2008.

9 BVerfG, 2.3.2010, 1 BvR 256, 263, 586/08 = BVerfG Official Case Reports E 125, 260. Abbreviated English version available at <www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html>.

10 BVerfG, *op. cit.* (n. 9), annot. 218 (English version).

11 BVerfG, *op. cit.* (n. 9), annot. 218 (original German version). This sentence was not translated in the abbreviated English version of the ruling.

12 A. Roßnagel, "Die ‚Überwachungs-Gesamtrechnung' – Das BVerfG und die Vorratsdatenspeicherung", (2010) 63(18), *Neue Juristische Wochenschrift (NJW)*, 1238–1242; A. Roßnagel et al., "On the Introduction of a Surveillance Calculus in Germany", Policy Paper, *Forum Privacy and Self-determined Life in the Digital World*, April 2022, <https://publica-rest.fraunhofer.de/server/api/core/bitstreams/47c4f3a8-73d4-405b-806f-072f4aa9c1bb/content>.

13 Originally, this approach leaned on the doctrine of "chilling" effects of state surveillance powers which are presumed to deter ("chill") citizens from exercising their rights and freedoms for fear of legal repercussions. The various aspects of that doctrine, including its weaknesses, are discussed, e.g., by J.W. Penney, "Understanding Chilling Effects", (2022) 106(3), *Minnesota Law Review*, 1451–1530.

14 The extremely low number of remote computer searches in police practice has been documented, for example, in an evaluation of these statutory powers carried out by the Federal Criminal Police Office of Germany (BKA) in the years 2009–2014; for more details, see H.-J. Albrecht & R. Poscher, *Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes*, BT-Drucksache 18/13031 of 23.06.2017, <https://dserver.bundestag.de/btd/18/130/1813031.pdf>.

15 Cf., e.g., J.-B. Maillard, "European Union", in: B. Vogel & J.-B. Maillard (eds.), *National and International Anti-Money laundering Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection*, 2000, pp. 71–155.

16 These include, *inter alia*, information on citizens' bank and credit card accounts (inventory data) as well as detailed records of bank

Dr. Dr. h.c. Michael Kilchling
Senior Researcher, Max Planck Institute for the Study of Crime, Security and Law, Public Law Department, Freiburg/Germany

Dr. Sabrina Ellebrecht
Senior Researcher, Max Planck Institute for the Study of Crime, Security and Law, Public Law Department, Freiburg/Germany

and credit card transactions, smart payments, cash transactions (above a certain limit), content data, etc. For a comprehensive analysis of all the various powers public agencies have to access and process the retained data, see C. Kaiser, *Privacy and Identity Issues in Financial Transactions: The proportionality of the European anti-money laundering legislation*, dissertation University of Groningen, 2018, <https://research.rug.nl/en/publications/privacy-and-identity-issues-in-financial-transactions-the-proport/2018>; L.M. Landerer, *Massenüberwachung von Finanzdaten. Die Geldwäschebekämpfung unter der Sicherheitsverfassung*, 2025.

17 Cf., e.g., E. Orrù, "The European PNR framework and the changing landscape of EU-security", *Verfassungsblog – On Matters Constitutional*, 21 December 2021, <https://verfassungsblog.de/os3-pnr/.>

18 With Regulation (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 2024/1624, new and further tightened elements of money laundering control will enter into force in July 2027, referred to by Tosza as silent expansion of the administrative AML control regime; S. Tosza, Enforcement of international sanctions as the third pillar of the anti-money laundering framework. An unannounced effect of the AML reform and the Sanctions Directive, 2024, *New Journal of European Criminal Law*, 15(3), pp. 336–356.

19 In German terminology and doctrine, 'basic rights' (*Grundrechte*) is used as a synonym for fundamental/human rights.

20 For more details, see, e.g., G. Letsas, "Proportionality as Fittingness: The Moral Dimension of Proportionality", (2018) 71(1) *Current Legal Problems*, 53–86; E. Orrù & R. Poscher, *Conceptions of Data Protection and Privacy. Legal and philosophical perspectives*, 2025.

21 Cf. M. Löffelmann, *Überwachungsgesamtrechnung und Verhältnismäßigkeitsgrundsatz*, 2022; *id*., "Eingriffsintensität und Eingriffsschwelle. Eine Formel für den Gesetzgeber", (2023) *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)*, 92–96; *id*., "Die Überwachungsgesamtrechnung", (2024) *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)*, 18–22.

22 Suggested readings include, e.g., D. Lyon, *Surveillance Studies: An Overview*, 2012; *id.*, *Surveillance Studies: A Very Short Introduction*, 2024, and the contributions provided in D. Wright & R. Kreissl, *Surveillance in Europe*, 2015.

23 Cf., e.g., S. Altwicker-Hármori et al., "Measuring Violations of Human Rights – An Empirical Analysis of Awards in Respect of Non-Pecuniary Damage under the European Convention for Human Rights", 2016, 76(1) *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV)*, 1–51, <www.zaoerv.de/76_2016/76_2016_1_a_1_52.pdf>.

24 Cf., e.g., D. Wright & P. de Hert, *Privacy Impact Assessment*, 2012.

25 Cf., e.g., P. de Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessment", in: D. Wright & P. de Hert (eds.), *Privacy Impact Assessment*, 2012, pp. 33–76; J. Milaj, "Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance", (2016) 30(3) *International Review of Law, Computers & Technology*, 115–130; G. Malgieri & C. Santos, "Assessing the (severity of) impacts on fundamental rights", (2025) 56 *Computer Law & Society Review: The International Journal of Technology Law and Practice*, 106113, <https://www.sciencedirect.com/science/article/pii/S0267364925000081>.

26 Cf., e.g., J. Milaj, *op. cit.* (n. 25).

27 Cf., e.g., M.-H. Maras, "The economic costs and consequences of mass communications data retention: Is the data retention directive a proportionate measure?", 2012, 33(2) *European Journal of Law and Economics*, 447–472.

28 D. Wright & C.D. Raab, "Constructing a surveillance impact assessment", 2012, 28(6) *Computer Law and Security Review*, 613–626.

29 According to Sajfert, their quality sometimes amounts to little more than "lip service"; J. Sajfert, *Resolving Legal Conflicts Between Data Access Investigative Measures and Data Protection Law in the EU. The case for quantitative data and balancing*, dissertation Université du Luxembourg, Faculty of Law, Economics and Finance, and Vrije Universiteit Brussel, Faculty of Law and Criminology, p.4, <https://orbilu.uni.lu/handle/10993/60157>.

30 For more details, see, e.g., R. Poscher & M. Kilchling, "Wie lässt sich die Überwachung der Bürgerinnen und Bürger messen? Pilotprojekt zur Messung der Überwachung in Deutschland", (2022) *Deutsche Richterzeitung* (*DRiZ*), 98–101; J. Milaj, *op. cit.* (n. 25); G. Malgieri & C. Santos, *op. cit.* (n. 25).

31 For more details, see Malgieri & Santos, *op. cit.* (n. 25).

32 For theoretical analyses of system-inherent problems of measurement in the context of the proportionality concept, see R. Poscher, "§ 3 – The Basic law as a constitution of proportionality balance", in: M. Herdegen et al. (eds.), *Constitutional Law in Germany. A Handbook in Transnational Perspective*, 2025; *id*., "What would it take? The potential and limits of proportionality analysis in law", (2025) 16(3) *Jurisprudence*, 443–476.

33 Bäcker collates all of them into four basic levels of intensity: low, medium, high, and highest: M. Bäcker, "§ 28 – The security constitution", in: M. Herdegen et al. (eds.), *Constitutional Law in Germany. A Handbook in Transnational Perspective*, 2025, annot. 25.

34 Judge Schluckebier, BVerfG, *op. cit.* (n. 9), annot. 311–314.

35 Judge Eichberger, BVerfG, *op. cit.* (n. 9), annot. 343.

36 Judge Schluckebier, BVerfG, *op. cit.* (n. 9), annot. 314.

37 Löffelmann therefore speaks of "*Begriffssynkretismus* [terminological syncretism]"; M. Löffelmann, "Datenerhebung aus dem „Smart Home" im Sicherheitsrecht", (2020) *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)*, 244–250.

38 It is likely that additional descriptive categories will have to be created for future cases.

39 Based on similar considerations, Roßnagel, (2010) NJW, *op. cit.* (n. 12), 1242 launched the idea of a "double proportionality test".

40 See above, II.1.

41 For a list of relevant projects, see Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht (MPI-CSL), *Überwachungsgesamtrechnung für Deutschland. Pilotstudie basierend auf der wissenschaftlichen Evaluation ausgewählter Überwachungsbefugnisse der Sicherheits- und Strafverfolgungsbehörden – Band 1*, 2025, p. 10; <https://pure.mpg.de/rest/items/item_3649030_9/component/file_3649042/content>.

42 Germany's architecture of security agencies is rather diverse. Responsibilities are distributed among 18 police agencies (2 federal and 16 state police forces), 25 prosecution divisions (organised alongside the jurisdiction of the 24 higher state courts, plus the Federal Attorney General who has primary jurisdiction in selected types of cases), 19 intelligence services (3 federal and 16 state agencies), and 4 customs agencies (Customs Criminal Office, Customs Investigations Bureau, Financial Intelligence Unit – FIU, Central Office for Sanctions Enforcement). With the exception of the prosecution sector, to which the German Code of Criminal Procedure applies, all other agencies act under their own sectoral laws, which are formally and substantively quite diverse.

43 <https://csl.mpg.de/815178/what-is-the-current-state-of-germany-s-security-laws>.

44 As of 2024.

45 Domestic surveillance powers exclusively. (Trans-)national

operations carried out by foreign agencies as well as data generated abroad and later shared with German agencies are not included. For conclusions drawn from the EncroChat, SkyECC and ANOM cases, see M. Lassalle and S. Lannier, "EncroChat – A Judicial Chronology"; and T. Wahl, "What Remains of the *ordre public* in Transnational Surveillance?" (both contributions are in this issue); as well as S. Gless, "Heiligt der Zweck die Mittel 2.0?" (2026), 144 *Schweizerische Zeitschrift für Strafrecht (ZStrR),* 80–107.

46 The urls will be: <https://surveillance-barometer.de> and <https://surveillance-barometer.eu>.

47 This exclusive focus on abstract parameters follows from the methodological limitation that the circumstances of individual surveillance operations could be collected by means of a case-by-case (file) analysis only.

48 For a complete inventory of the 18 variables and their composition, see MPI-CSL, *op. cit*. (n. 41); *id*., *Überwachungsgesamtrechnung für Deutschland. Pilotstudie basierend auf der wissenschaftlichen Evaluation ausgewählter Überwachungsbefugnisse der Sicherheits- und Strafverfolgungsbehörden – Band 2: Manual,* 2025, <https://pure.mpg.de/rest/items/item_3649032_9/component/file_3649041/content>.

49 NI = S – S (0.15 * M / 10) and NI >=1 (see below, Figure 2).

50 For more details, see MPI-CSL, *op. cit.* (n. 41), *id*., *op. cit.* (n. 48).

51 Updates and amendments for 2023 and 2024 have almost been completed, too.

52 For more details, see MPI-CSL, *op. cit.* (n. 41), pp. 52 et seq.

53 K. Hesse, *Der unitarische Bundesstaat*, 1962, p. 9; K. Graulich, "Das Handeln der Polizei- und Ordnungsbehörden zur Gefahrenabwehr", in: M. Bäcker et al. (eds.), *Handbuch des Polizeirechts*, 7th ed. 2021, pp. 341–823 (p. 372).

54 For the purpose of the Barometer, it matters whether a high- or very high-intensity measure is carried out 10 or 20 times; however, it is irrelevant whether a standard measure of (very) low intensity has 100,001, 100,010, or 100,500 counts.

55 In total, more than 50 different types and techniques of surveillance were identified; for more details, see MPI-CSL, *op. cit.* (n. 41), pp. 25 et seq. (table 2).

56 See above, note 42.

57 BVerfGE 125, 260, 344; *op. cit.* (n. 9).

58 For further details, see MPI-CSL, *op. cit.* (n. 41), pp. 16 et seq.

59 See above, I.

60 Sec. 101b StPO.

61 Sec. 88 BKAG.

62 E.g., Sec. 90 Police Act for Baden Württemberg, Art. 52 Bavarian Police Act, etc. For a comprehensive list, see MPI-CSL, *op. cit.* (n. 41), pp. 18 et seq. (table 1).

63 This provision obliges all prosecution offices (state and federal) to provide detailed annual statistics on the following covert measures of surveillance ordered and carried out, together with some further statutorily specified details about the circumstances of their execution: surveillance of telecommunication, remote computer search, capture of telecommunication traffic data (meta data), capture of usage data in respect of digital services, and acoustic surveillance of private premises. Meanwhile, data about telephone tapping are available for a long time period since 2000; the collection of others started later, in particular those relating to measures which were introduced only a few years ago.

64 Cf. <www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html>.

65 According to Sajfert, *op. cit.* (n. 29), ensuring transparency is the one of the most challenging fundamental principles for the EU as a whole.

66 Art. 28 of Directive 2012/29/EU of 25 October 2012 on minimum standards on the rights, support and protection of victims of crime, OJ L 315, 14.11.2012, 57.

67 Art. 14 of Directive 2013/40/EU of 12 August 2013 on attacks against information systems, OJ L 218, 14.8.2013, 8.

68 Art. 28 of Directive (EU) 2024/1260 of 24 April 2024 on asset recovery and confiscation, OJ L. 2024/1260.

69 Specified in Art. 28 lit. a-k.

70 Art. 9 of Directive (EU) 2024/1640 of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 2024/1640.

BEYOND THE FOCUS

The Poland–Indonesia Treaty on Mutual Legal Assistance in Criminal Matters

Forging Legal Ties across Continents

Lukasz Zygmunt*

This article provides an overview of the key provisions of the Poland-Indonesia Treaty on Mutual Legal Assistance in Criminal Matters. The Treaty was signed on 19 September 2025 and opens a new chapter in the relationship between both countries with regard to combating crime. It also includes modern forms of assistance, such as the possibility of conducting hearings by videoconference. Robust provisions on data protection and confidentiality are among the safeguards for the individual.

I. Introduction

On 19 September 2025, two countries with remarkably similar flags – the Republic of Poland and the Republic of Indonesia – marked a new chapter in their long-standing bilateral relations by signing the *Treaty on Mutual Legal Assistance in Criminal Matters* in Poland's capital Warsaw. The signing took place during the official visit of *Supratman Andi Agtas*, Minister of Law of Indonesia, at the invitation of *Waldemar Żurek*, Minister of Justice of Poland. The event held particular symbolic significance, as it coincided with the *70th anniversary of diplomatic relations* between the two nations.[1] The Treaty's signing was accompanied by a Joint Statement affirming the shared vision of both governments to strengthen cooperation in criminal justice, enhance institutional capacity, and promote mutual respect for sovereignty and the rule of law.

The relationship between the two countries has been characterised by a spirit of mutual respect and constructive engagement ever since diplomatic ties were first established on 19 September 1955. Both countries have evolved into increasingly significant regional actors, Poland within the European Union (EU) and Indonesia within the Association of Southeast Asian Nations (ASEAN).[2]

The idea of concluding a bilateral agreement was first conceived during bilateral consultations in 2019, at the initiative of the Ministry of Justice of the Republic of Poland. Negotiations were conducted through diplomatic channels and directly, and lasted two years. The negotiations were concluded during a meeting in Warsaw, Poland, on 12–13 June 2024.

The signed Treaty aims at facilitating cooperation between Poland and Indonesia in criminal matters through formalised procedures for mutual legal assistance (MLA). Both justice ministers agree that strengthening judicial cooperation is essential for addressing contemporary challenges, such as corruption, organised crime, and money laundering. The ministers have also expressed their intention to initiate consultations on a bilateral extradition treaty.

II. Objectives and Scope of the Treaty

The Poland-Indonesia MLA Treaty[3] is designed to enhance cooperation between the judicial authorities of both countries in investigating, prosecuting, and preventing criminal offences. It provides a comprehensive legal framework for requesting and granting mutual legal assistance, while ensuring that the fundamental principles of sovereignty, equality, human rights, and due process are respected.

Under Article 1, the Parties commit to assisting one another in criminal cases falling within the jurisdiction of the requesting country. The assistance extends to the collection and exchange of evidence, locating suspects or witnesses, serving judicial documents, executing searches and seizures, taking testimony, and freezing or confiscating the proceeds of crime. It is important to note that the Treaty does not cover extradition, which is expected to be regulated by a separate instrument. The transfer of sentenced persons, the transfer of criminal proceedings, and the execution of penal judgements are also excluded from its scope.

Each Party designates a Central Authority responsible for communication and coordination: for Poland, this is the *Minister of Justice*; for Indonesia, this is the *Minister of Law*. This direct channel is intended to eliminate bureaucratic delays and ensure transparency and efficiency when processing requests.

III. Procedural Framework

The Treaty sets out clear procedural standards for the transmission and execution of MLA requests. Requests must be made in writing and translated into English before being transmitted through the respective Central Authorities. In urgent cases, electronic communication is permitted, provided authenticity can be verified.

The Treaty specifies which content must be included in an MLA request, such as the identity of the requesting authority, details of the case, the legal basis, and information on the evidence sought. The principle of proportionality is emphasised (Art. 10): both Parties must assess whether the request is necessary and proportionate for the purposes of the proceedings. In particular, the competent authority issuing a request and the central authority of the requesting Party are required to assess whether the issuance of the request is necessary and proportionate for the purposes of the proceedings, on a case-by-case basis. Even if this assessment results in a decision to proceed, the central authority of the requested Party remains entitled to raise concerns about the necessity or proportionality of the request. In such circumstances, the Treaty provides for a consultation procedure (Art. 10(2)), whereby the central authorities may consult on the execution of the request. This could potentially lead to the request being withdrawn, or executed subject to specified conditions. Although this procedure is voluntary, it is difficult to envisage a request being refused

without prior consultations having taken place, given the framework of good international cooperation. In any event, if the request is ultimately refused, the requesting Party must be informed of the reasons for the refusal (Art. 12(3)).

Requests may be refused on either mandatory (Art. 12) or optional (Art. 13) grounds. Mandatory refusal applies in the following cases:

- The execution would prejudice national sovereignty, security, public order or national interest (Art. 12 (1)(a));
- The offence is political (Art. 12 (1)(b)) or military (Art. 12 (1)(c)) in nature;
- There are concerns about discrimination (Art. 12 (1)(d))4 or double jeopardy (Art. 12 (1)(e)).

Optional refusal may occur in the following instances:

- The offence is not recognised under the requested Party's domestic law (Art. 13 (1)(a))5;
- The offence has been committed by a person who, under the national law of the Requested Party, is not subject to criminal liability because of their age (Art. 13 (1)(b))
- The offence involves the death penalty without assurances against its application (Art. 13 (1)(c)).
- The assistance sought could impose an excessive burden on the resources of the Requested Party and the Requesting Party refused to cover them (Art. 13 (1)(d)).

In the latter case, the Parties may agree on special rules of covering costs other than the general rules of costs sharing provided in Art. 25 (1) and (2) of the Treaty.

The Treaty also stressed in Art. 13(2), that the legal assistance in criminal matters may not be refused solely on the grounds of the secrecy of a bank or another financial institution.

The agreement places great emphasis on the protection of personal data. To safeguard personal rights, the Treaty incorporates detailed provisions on data protection and confidentiality in connection with the execution of a request (Art. 7). Shared information can only be used for the purposes specified in the request, and both Parties must protect data against unauthorised disclosure or misuse. This aligns the Treaty with modern international privacy standards, thereby reinforcing its compatibility with both EU law and Indonesian data protection principles. The data protection mechanism of the Treaty takes into account the provisions of Directive (EU) 2016/680.[6]

The data protection safeguards imposed by Art. 7 include the following:

- Obligation for the Parties to ensure that personal data transmitted pursuant to the Treaty are used solely for the purposes for which they were provided (Art. 7. (1));
- Data transfer exclusively by the authorities competent to do so (Art. 7 (2)(a));
- Data storage only for the period necessary for the aforementioned purposes, as determined in accordance with domestic regulations governing the data retention period, combined with the obligation to destroy the data no longer needed without delay (Art 7 (2)(f).

Art. 7(2)(b) requests the receiving Party, at the request of the transmitting Party, to provide information on how the transmitted data have been used, thereby enabling mutual oversight by the Parties of such processing. Article 7 also safeguards the rights of data subjects by guaranteeing their right to be informed about the transferred data and their right of access to personal data relating to them. Data subjects also have the right to request the rectification or erasure of such data and to have access to an effective legal remedy (Art.7 (4)).

IV. Forms of Assistance and Costs

The Treaty encompasses a wide range of cooperation mechanisms (Art. 9(1)(a-j)), including:

- The locating and identifying of persons, property, or assets;
- The serving of judicial documents;
- The taking of witness statements and expert evidence, including through videoconference hearings;
- The execution of searches and seizures;
- The freezing, confiscation, or forfeiting of proceeds and instrumentalities of crime;
- The temporary transfer of persons in custody for testimony or cooperation in investigations, and initiation of criminal proceedings upon request.

The list of cooperation measures is not exhaustive. The Treaty also provides for any other form of legal assistance, as permitted by the national law of the requested Party.

Notably, the Treaty facilitates videoconference hearings (Art. 17), reflecting the modernisation of cross-border legal cooperation and the use of digital tools in criminal proceedings. The introduction of the possibility of executing requests for legal assistance through videoconference hearings, together with the detailed regulation of this procedure, aims to reduce costs, facilitate judicial cooperation between geographically distant states, and encourage judicial authorities to make broader use of this form of cooperation. Procedural safeguards ensure that such hearings respect national laws and the rights of defendants and witnesses. This is guaranteed by the

fact, that a videoconference hearing shall be conducted directly by the judicial authority of the requesting Party in the presence of the judicial authority of the requested Party (Art. 17 (4)). Where requested by either Party or the person to be heard, an interpreter shall assist in the hearing (Art. 17 (3)). Upon the requesting Party's request, the requested Party shall draw up and transmit the minutes from a videoconference hearing (Art. 17(6)).

Provisions on the temporary transfer of persons in custody (Art. 19) and the return of seized items (Art. 23) demonstrate the Treaty's comprehensive scope, which covers not only evidence gathering but also post-investigation procedures. The Treaty also allows for cooperation in cases involving tax, customs, and financial crimes, thereby aligning with global efforts against money laundering and illicit financial flows.

Under Art. 25 of the Treaty, the general rule is that the Requested Party bear the costs of executing an MLA request within its territory. However, certain expenses – such as interpreter fees, expert testimony, travel costs for witnesses, and the transfer of detained persons – are to be borne by the Requesting Party. This cost-sharing ensures fairness and encourages cooperation even in resource-intensive cases.

V. Implementation and Outlook

The Treaty enters into force 30 days after both countries have completed their domestic ratification procedures and remains in force indefinitely. As far as Poland is concerned, the Prime Minister presented to the Polish Parliament (*Sejm*) a draft law on the ratification of the Treaty on 13 January 2026. On 20 January 2026, the draft was submitted for its first reading in committees.[7] Following the Parliament's consent (or approval by referendum approval), the President of the Republic of Poland will formally ratify the Treaty and sign the instrument of ratification.[8]

Once into force, the Treaty may be terminated with six months' notice, but termination does not affect ongoing proceedings. This treaty design provides both stability and predictability, which are essential features in an agreement of international criminal cooperation.

As the treaty was signed in September 2025, and still needs to be ratified, a comprehensive evaluation of its impact will require time. Nevertheless, its provisions already represent a significant step towards enhanced international cooperation. In this context, it should be born in mind that, cooperation to date has been conducted in the absence of a bilateral agreement and relies solely on the international principle of reciprocity. This has proved insufficient. The execution of requests submitted by the judicial authorities of Poland (Polish courts and public prosecutors) by the Indonesian authorities has often been time-consuming. Indonesia requires that requests and all accompanying documents be translated into the Indonesian language, which significantly increased the costs of proceedings. Moreover, due to the limited number of qualified translators, the preparation of requests was frequently delayed, and the quality of the translations was questioned in some cases by the Indonesian side. The new Polish-Indonesian MLA Treaty now clearly defines the requirements applicable to requests for legal assistance, including their form, content, and accompanying documents (Art. 11). This is intended to reduce the number of requests rejected for purely formal reasons with the result of non-execution.

Lukasz Zygmunt
Public Prosecutor, District Public Prosecutor's Office Lublin-North in Lublin, Poland
Member of the European Commission's Expert Group on EU Criminal Policy

* The author was former inaugural Head of the Extradition Division, Department of International Cooperation and Human Rights, Polish Ministry of Justice. In this function, he had the privilege of participating in the third round of the MLA treaty negotiations between Poland and Indonesia, which were combined with consultations on extradition. This article exclusively expresses the views of the author and cannot be attributed to the institution(s) that employs or employed him.

1 Cf. News, "Signing of the Agreement between the Republic of Poland and the Republic of Indonesia on Mutual Legal Assistance in Criminal Matters", 19 September 2025, Website of the Republic of Poland, <https://www.gov.pl/web/indonesia-en/signing-of-the-agreement-between-the-republic-of-poland-and-the-republic-of-indonesia-on-mutual-legal-assistance-in-criminal-matters> accessed 16 March 2026.

2 Regarding how mutual legal assistance in criminal matters can developed within and between the ASEAN and the EU, see A. Aguinaldo, *East Meets West – Development of Mutual Legal Assistance in Criminal Matters between and within the Association of Southeast Asian Nations and the European Union*, Nomos 2021.

3 Cf. <https://orka.sejm.gov.pl/Druki10ka.nsf/0/8BED1997654C-7C5DC1258D85005EFBBA/%24File/2161.pdf> accessed 16 March 2026.
4 The Treaty mentions race, sex, age, disability, religion, national, ethnic or social origin, wealth, birth or other status or on account of their political or other views as grounds for discrimination
5 Double criminality requirement.
6 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, *OJ L 119, 4.5.2016, 89*. The Directive was implemented into Polish law by the Act of 14 December 2018 on the protection of personal data processed in connection with the prevention and combating of crime (consolidated text: Journal of Laws 2023, 1206).
7 The Committee on Foreign Affairs and the Committee on Justice and Human Rights. The legislative process is available on the Parliament's website: <https://www.sejm.gov.pl/Sejm10.nsf/PrzebiegProc.xsp?id=79A47F5CA4013B1FC1258D85005F9A39&SessionID=412C58AE88B52D475094FCC40CCE48FB0CFAC9A0> acessed 16 March 2026.
8 This is a constitutional prerogative of the President (Art. 133 of the Constitution of the Republic of Poland).

Neues zum Rechtshilfeverkehr zwischen Deutschland und Taiwan

Ralf Riegel und Teresa Steiger*

In 2013, the German Institute Taipei and the Taipei Representative Office in Germany reached a joint declaration on the transfer of convicted persons and on cooperation in the enforcement of criminal judgments → R. Riegel and F. Fülle, "Vollstreckungshilfe zwischen Deutschland und Taiwan auf neuer Grundlage", (2016) *eucrim*, 61–64). This declaration led to the successful transfer of a number of prisoners and the enforcement of sentences. In 2023, the German Institute Taipei and the Taipei Representative Office in Germany signed a further declaration on cooperation in the field of mutual legal assistance in criminal matters, which has been applicable since 11 June 2025. This article outlines the basis for cooperation between Germany and Taiwan and explains the content of the joint agreement. The German version of the joint declaration is reproduced at the end.

I. Einleitende Bemerkungen

Die internationale Zusammenarbeit in Strafsachen ist von immenser Bedeutung für die erfolgreiche Bekämpfung und Verfolgung von grenzüberschreitender Kriminalität. Die fortschreitende Globalisierung und der technologische Fortschritt gehen mit einer zunehmenden Internationalisierung der Kriminalität einher. Rechtshilfe ist dabei notwendig, um auf fremdem Territorium ermitteln zu können oder Ermittlungen durchführen zu lassen. Sie ist damit Teil der gegen die verfolgte Person durchgeführten Strafverfolgung. Eine gut funktionierende internationale strafrechtliche Zusammenarbeit ermöglicht die effektive Durchsetzung nationaler Strafverfolgungsansprüche. Dies gilt aber nur, wenn es in der gesamten Welt keine „sicheren Häfen" gibt, also keine Staaten, bei denen Straftäterinnen und Straftäter davon ausgehen können, dass sie Ermittlungen nicht unterstützen werden und eine Auslieferung von vornherein ausgeschlossen ist.

Das Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) ermöglicht in § 2 Abs. 1 und § 59 Abs. 1 eine umfassende vertragslose Zusammenarbeit. Vereinfacht wird eine solche, wenn es allgemeine, von beiden Seiten vereinbarte und angewandte Regelungen gibt, die eine Zusammenarbeitspflicht begründen und wiederkehrende grundlegende Fragen lösen. Deutschland hat mit Taiwan eine gemeinsame Absprache über die Zusammenarbeit hinsichtlich justizieller Rechtshilfe in Strafsachen getroffen, die seit 2025 anwendbar ist. Der Beitrag widmet sich in den ersten beiden Kapiteln der Frage, ob eine Absprache mit Taiwan völkerrechtlich zulässig ist und unter welchen Voraussetzungen, insbesondere im Hinblick auf den komplexen politischen Status Taiwans, sie zustande kommen kann. In einem dritten Teil folgt neben einem Überblick über den zum Verlauf auch der vorangegangen Verhandlungen eine erläuternde Zusammenfassung des Inhalts.

II. Die Rechtsstellung Taiwans

Die Stellung Taiwans wird zunächst aus historischem sowie aus völkerrechtlichem Blickwinkel betrachtet. Davon zu unterscheiden ist die im Anschluss erfolgende rechtshilferechtliche Einordnung, die für die grenzüberschreitende strafrechtliche Zusammenarbeit maßgeblich ist.

1. Historische Entwicklung

Die Insel Taiwan gehörte von 1683 bis 1895 zum chinesischen Kaiserreich. Von 1895 bis 1945 war sie japanische Kolonie. 1912 wurde die Republik China auf dem chinesischen Festland ausgerufen. 1945 erfolgte die Rückgabe Taiwans von Japan an China (seinerzeit noch Republik China). 1949 zog sich die im chinesischen Bürgerkrieg geschlagene Regierung *Chiang Kai-sheks* nach Taiwan zurück und führte auf dem Gebiet der Insel Taiwan die Republik China fort, während auf dem übrigen Staatsgebiet die unter der Führung *Mao Tsetungs* die Volksrepublik China gegründet wurde.[1]

Die Republik China (im Folgenden zur besseren Unterscheidung: Taiwan) vertrat in den nächsten Jahren die gesamtchinesischen Interessen international. Sie stellte bis 1971 die Delegation bei den Vereinten Nationen und war ständiges Mitglied des UN-Sicherheitsrats. In der Folgezeit brachen immer mehr Staaten ihre diplomatischen Beziehungen zu Taiwan ab. Aktuell wird Taiwan nur von sechs anderen Staaten der Welt vollumfänglich als eigener Staat anerkannt.

2. Völkerrechtliche Entwicklung

1971 entwickelte die Volksrepublik China die Ein-China-Politik, die konsequent dafür sorgt, dass China auf dem internationalen Parkett ausschließlich von der Volksrepublik vertreten wird unter der Prämisse, dass Taiwan lediglich Teil dieses Staates sei.

Die Vollversammlung der Vereinten Nationen beschloss in ihrer Resolution 2578 im selben Jahr:[2]

> „(…) all die Rechte der Volksrepublik China instandzusetzen und die Vertreter ihrer Regierung als die einzigen legitimierten Vertreter Chinas in den Vereinten Nationen anzuerkennen und von nun ab die Vertreter Chiang Kai-sheks von dem Platz zu entfernen, den sie zu Unrecht in den Vereinten Nationen und all ihren Organisationen einnehmen."

Taiwan verlor in der Folge seinen Sitz in internationalen Organisationen.

Die Volksrepublik China legt die Resolution der Vereinten Nationen derart aus, als werde Taiwan dort als ein „abtrünniger Teil der Volksrepublik" betrachtet. Sie erkennt eine Selbständigkeit nicht an.[3] Andere Staaten gehen in ihrer Interpretation der Resolution nicht so weit. Sie festige den Status der Volksrepublik China bei den Vereinten Nationen, erwähne aber im Wortlaut nicht Taiwan und ändere nichts an der Souveränität Taiwans.[4] Taiwan selbst sieht sich als eigenständige Nation, hat aber formal keine Unabhängigkeit erklärt. Aktuell unterhält das Land zu 12 Staaten vollständige diplomatische Beziehungen.[5]

Die Bundesrepublik Deutschland pflegt keine formalen diplomatischen Beziehungen zu Taiwan. Die Bundesregierung hat sich der Ein-China-Politik angeschlossen, die nur die Volksrepublik China diplomatisch anerkennt, und unterhält zu Taiwan eine sogenannte Wertepartnerschaft.[6]

3. Taiwan als stabilisiertes De-facto-Regime

Damit ein Herrschaftsverband den rechtlichen Status eines Staates erlangt, bedarf es erstens eines Staatsgebiets, zweitens eines Staatsvolks und drittens einer durchsetzbaren staatlichen Hoheitsgewalt.[7] All dies ist für Taiwan zutreffend. Diskutiert wird, ob es als vierte notwendige Voraussetzung einer Völkerrechtssubjektivität auch der Anerkennung durch andere Staaten und internationale Organisationen bedarf.[8] Eine solche wird als Folge des Ein-China-Konzepts zu verneinen sein.

Zumindest für die effektive praktische Zusammenarbeit der grenzüberschreitenden Strafverfolgung ist jenseits einer juristischen Diskussion jedoch keine Anerkennung notwendig. Denn dafür reicht es aus, wenn Taiwan als stabilisiertes De-facto-Regime angesehen werden kann.

Der Begriff des De-facto-Regimes knüpft an die effektive Beherrschung eines Territoriums durch eine strukturierte und organisierte Gemeinschaft an, die sich als unabhängig bezeichnet, deren Zusammenschluss aber aktuell nicht als eigenständiger Staat anerkannt wird. Ein Regime dieser Art verfügt über eine dauerhafte hoheitsförmige Gewalt und über eine Stabilität, die jener eines Staats gleichkommt.[9] Es entsteht oft bei einer Loslösung oder Abspaltung von einem Mutterstaat.[10]

Besteht eine dauerhafte effektive Herrschaft, kann dem Regime unabhängig von einer formalen Anerkennung Völkerrechtssubjektivität nach dem Effektivitätsprinzip zuwachsen. In diesen Fällen spricht man von einem „stabilisierten De-facto-Regime". Ein solches Regime erfüllt die Voraussetzungen der Staatlichkeit auf dem von ihm beherrschten Gebiet, so dass es von Drittstaaten nicht mehr als rechtliches Nullum betrachtet werden kann.[11]

Die Merkmale eines stabilisierten De-facto-Regimes treffen auf Taiwan zu. Diesen Status hat es inne, auch wenn Taiwan von der Mehrheit der Staaten aus politischen Gründen nicht anerkannt wird. Entscheidend in diesem Zusammenhang ist vielmehr die Tatsache, dass Taiwan tatsächlich und dauerhaft die effektive und befriedete Herrschaftsgewalt über die Insel ausübt. Dadurch hat Taiwan partielle Völkerrechtssubjektivität erlangt.[12]

4. Stellung Taiwans nach dem IRG

Das IRG erlaubt eine Zusammenarbeit in Strafsachen mit anderen „Staaten".[13] Der Begriff des Staates in diesem Sinne ist in diesem Zusammenhang so auszulegen, dass er auch stabilisierte De-facto-Regime umfasst.

In einem Beschluss vom 26. August 2022 hat das OLG Frankfurt die Anordnung von Auslieferungshaft gegen eine von Taiwan verfolgte Person abgelehnt und ausgeführt, eine ausreichende Wahrscheinlichkeit der Zulässigkeit der Auslieferung an Taiwan bestehe nicht. Das Auswärtige Amt und das Bundesamt für Justiz hätten die Fragen, ob es sich bei Taiwan um einen souveränen Staat handele, der Zusicherungen abgeben könne, nicht in der für eine Haftentscheidung gebotenen Geschwindigkeit beantworten können.[14] Kritisch ist der Beschluss des OLG dahingehend zu beurteilen, dass die Frage, ob Taiwan ein Staat im Sinn des IRG ist und Zusicherungen belastbar sind, eine vom zuständigen Gericht zu entscheidende Rechtsfrage auf der Zulässigkeitsebene ist. Die Bewilligungsbehörden (hier: Auswärtiges Amt und Bundesamt für Justiz) entscheiden nach Feststellung der Zulässigkeit allein über die außenpolitische Bewertung, die anderen Regeln folgt.

Der Wortlaut der Normen des IRG spricht eher für das klassische Verständnis von Völkerrechtssubjektivität, das eine Anerkennung eines Landes als Staat voraussetzt. Dafür spricht auch die historische Auslegung: Schon § 1 und § 41 des Deutschen Auslieferungsgesetzes (DAG) vom 23. November 1929 nutzten den Terminus „Staat". Zu der Zeit gab es keine Überlegungen zu einer erweiterten Auslegung des Begriffes im Völkerrecht. Gestützt wird dies durch Artikel XV des ersten und lange Zeit einzigen deutschen Auslieferungsvertrages aus dem Jahr 1872 mit Großbritannien, der die Anwendbarkeit explizit auf „die Kolonien und auswärtigen Besitzungen Ihrer Großbritannischen Majestät" erstreckte und keine gesonderte Bewertung territorialer Eigenständigkeit vorsah.[15] Zu berücksichtigen ist allerdings, dass sich die Völkerrechtslehre seit diesen Zeiten erheblich weiterentwickelt hat und die gegenwärtigen Gegebenheiten den Situationen von 1872 oder 1929 nicht mehr entsprechen. Der historischen Betrachtung kommt gerade hier nur geringe Bedeutung zu.

Systematisch kann darauf verwiesen werden, dass die Grundnorm des § 1 IRG gerade nicht von einem Staat, sondern von der Zusammenarbeit mit dem Ausland spricht und damit den Fokus genereller auf fremdes Territorium legt.

Entscheidend ist die teleologische Auslegung des Staatsbegriffs im IRG. Zwischenstaatliche Zusammenarbeit im Bereich des Strafrechts basiert auf drei Prinzipien: außenpolitische Gegenseitigkeit, länderübergreifende Repression und Prävention. Taiwan leistete auf Ersuchen aus Deutschland bereits vor der Absprache sonstige Rechtshilfe; die Gegenseitigkeit wird nur gewahrt, wenn Deutschland seinerseits Rechtshilfe leistet. Die Aufklärung grenzüberschreitender Straftaten ist nur durch gemeinsame Anstrengungen möglich. Auf dem Gebiet eines stabilisierten De-facto-Regimes können ausschließlich Vertreter des Regimes Strafverfolgungsmaßnahmen durchführen. Ein solches Regime nicht zur Rechtshilfe zuzulassen würde bedeuten, dauerhaft auf einem Territorium einen verfolgungsfreien Raum, einen – im Rechtshilfeverkehr zu vermeidenden – sicheren Hafen zu schaffen. Die Prävention von Straftaten auch in Deutschland wird gestärkt, wenn es einen Verfolgungsdruck gibt. Aufgrund dieser, insbesondere auf Systematik und Sinn und Zweck der Norm beruhenden Überlegungen ist die Zusammenarbeit im Bereich der strafrechtlichen Rechtshilfe mit einem stabilisierten De-facto-Regime, mit Taiwan rechtlich möglich.[16]

III. Rechtshilfeverkehr mit Taiwan vor der Absprache

Im Verhältnis zu Taiwan lassen sich die rechtliche Grundlage und weitere Hinweise für die bilaterale Zusammenarbeit in Strafsachen der Anlage II, dem Länderteil der Richtlinien über den Verkehr mit anderen Staaten in strafrechtlichen Angelegenheiten (RiVASt) entnehmen. Demnach erfolgte der sonstige Rechtshilfeverkehr vor Wirksamwerden der Absprache vertraglos, das heißt, auf Grundlage der §§ 59 ff. IRG und des taiwanesischen Mutual Legal Assistance in Criminal Matters Act vom 2. Mai 2018.[17]

Der taiwanesische Mutual Legal Assistance in Criminal Matters Act folgt einer engen Definition von Rechtshilfe im Bereich des Strafrechts, d.h. Auslieferungen und der Transfer von verurteilten Personen sind hier nicht erfasst. Auch die Durchbeförderung von Zeugen fällt nicht darunter. Ermöglicht werden hingegen die Übermittlung strafrechtlich relevanter Dokumente, die Umsetzung von Einziehungs- und Beschlagnahmebeschlüssen, die Rückführung und die Teilung von Erträgen aus Straftaten und die Beschaffung von Beweisen. Letzteres lässt auch die Aufnahme von Zeugenaussagen, die Durchführung von Durchsuchungen und

Beschlagnahmen sowie die Herausgabe vorhandener Beweismittel zu. Es ist erlaubt, dass ausländische Beamte bei Befragungen anwesend sind oder an Zeugenbefragungen über Video teilnehmen. Die ersuchende Seite kann die Befragungen jedoch nicht selbst vornehmen. Ist Taiwan ersuchender Staat, sind die Behörden gemäß Article 32 des Mutual Legal Assistance in Criminal Matters Act an sämtliche taiwanesische Zusicherungen gebunden, die nicht gegen dortiges Recht verstoßen. Auch in Taiwan hat ein Vertrag zwischen Ländern oder ein Abkommen Vorrang vor dem nationalen Recht. Abkommen über die Rechtshilfe in Strafsachen können deshalb auch spezifische Kooperationsinstrumente beinhalten, die im nationalen Recht noch nicht vorgesehen sind.

IV. Die gemeinsame Absprache über sonstige Rechtshilfe mit Taiwan

1. Verlauf der Verhandlungen

Nachdem das Deutsche Institut Taipei und die Taipeh Vertretung in der Bundesrepublik Deutschland am 15. November 2013 im Bereich der Vollstreckungshilfe die Absprache über die Überstellung verurteilter Personen unterzeichnet hatten und diese erfolgreich in die Praxis umgesetzt wurde,[18] wurden im Dezember 2019 konkrete Überlegungen zu einer entsprechenden Absprache auf dem Gebiet der sonstigen Rechtshilfe angestellt. Aufgrund pandemiebedingter Verzögerungen konnten jedoch erst im Sommer 2021 Verhandlungen aufgenommen werden, die in die Unterzeichnung der Absprache zwischen dem Deutschen Institut Taipei und der Taipeh Vertretung in der Bundesrepublik Deutschland über die Zusammenarbeit auf dem Gebiet der justiziellen Rechtshilfe in Strafsachen am 23. März 2023 in Taipei mündeten (→nebenstehend abgedruckt auf Seiten 267–270).

Unter Beachtung der herausfordernden politischen Implikationen ging es im Rahmen der bilateralen Gespräche mit Taiwan darum aufzuklären, inwieweit die taiwanesischen Rechtsgrundlagen für die Rechtshilfe und die dortigen Verfahrensgarantien in Strafverfahren eine rechtsstaatliche Qualität der Zusammenarbeit gewährleisten. An einer solchen bestanden im Ergebnis keine Bedenken.

Der Abschluss eines förmlichen völkerrechtlichen Vertrages im Sinne von § 1 Abs. 3 IRG war nicht möglich (siehe oben I.2). Stattdessen konnte nur eine Absprache unterhalb der völkerrechtlichen Vertragsschwelle getroffen werden, die sich im Wesentlichen durch die Abgrenzung von rechtsverbindlichen völkerrechtlichen Verträgen definiert (vgl. § 72 Abs. 6 Gemeinsame Geschäftsordnung der Bundesministerien (GGO) i.V.m. § 4 der Richtlinien für die Behandlung völkerrechtlicher Verträge (RvV).

2. Inhalt der Absprache

Gemäß Ziffer I Abs. 1 der Absprache richtet sich die Zulässigkeit der Rechtshilfe nach dem jeweiligen nationalen Rechtshilferecht. Ziffer XIV Abs. 1 bestimmt, dass die Vornahme nach dem Recht des ersuchten Staates erfolgt. Die Absprache ändert also nicht das nationale Recht, sondern stellt zur Erleichterung der Anwendbarkeit dessen Inhalt im bilateralen Verhältnis klar.

Ziffer III benennt die zuständigen Behörden. Mit dem Bundesamt für Justiz auf deutscher und der Abteilung für internationale und Cross-Strait-Rechtsangelegenheiten des Justizministeriums Taiwan werden Zentralstellen benannt, die in Einzelfällen (Ziffer V Abs. 3, Ziffer XIII Abs. 4, Ziffer XIV Abs. 2) und bei allgemeinen Konsultationen (Ziffer XVII Abs. 1) miteinander kommunizieren sollen.

Ziffer IV Abs. 1 listet die notwendigen Inhalte von Rechtshilfeersuchen auf. Da es unterschiedliche chinesische Sprachformen gibt, ist es wichtig, nach Ziffer IV Abs. 2 eine Übersetzung von Ersuchen in traditionelles Chinesisch zu veranlassen.

Nach Ziffer V Abs. 1 in Verbindung mit Nr. 5 Abs. 2 RiVASt ist der diplomatische Geschäftsweg zwischen der Taipeh Vertretung in der Bundesrepublik Deutschland und dem Deutschen Institut in Taipeh vorgesehen. Zur Verfahrensbeschleunigung (Abs. 2) können Ersuchen zusätzlich (!) vorab zwischen den Zentralen Behörden übermittelt sowie erforderlichenfalls Anfragen betreffend Rechtshilfe auch in englischer Sprache unmittelbar zwischen den vorgenannten Behörden ausgetauscht werden.

Die Ziffern VI bis XI enthalten Regelungen zu einzelnen Maßnahmen. Inhaltlich orientiert sich dieser Teil am Europäischen Rechtshilfeübereinkommen und dessen Zweiten Zusatzprotokoll. Praktisch bedeutsam ist, dass Videovernehmungen durch eine Stelle des ersuchenden Staates durchgeführt werden können (Ziffer VII Abs. 1). Die Absprache verhält sich nicht dazu, ob nur Zeuginnen, Zeugen und Sachverständige oder auch beschuldigte Personen per Video vernommen werden können. Eine Art. 9 Abs. 8 2. ZP-EuRhÜbk entsprechende Regelung wurde nicht aufgenommen, obgleich sich Ziffer VII im Übrigen an dem Abkommen orientiert. Da sowohl das IRG als auch Art. 17 Abs. 2 des Mutual Legal Assistance in Criminal Matters Act eine solche Videovernehmung durch den ersuchten

Staat bei Zuschaltung des ersuchenden Staates nicht ausschließt, ist diese auch durch die Absprache abgedeckt. Ein weiteres praktisches Element ist, dass Ermittlungspersonen aus dem ersuchenden Staat bei Durchsuchungen anwesend sein können (Ziffer IX). Ziffer X erlaubt die Bildung gemeinsamer Ermittlungsgruppen, soweit das nach dem jeweiligen nationalen Recht möglich ist. § 61b Abs. 1 IRG setzt dafür das Vorliegen einer völkerrechtlichen Vereinbarung voraus. Beide Seiten gehen davon aus, dass diese Absprache dazu ausreichend sein kann.

Die Ziffern XII bis XIX enthalten allgemeine Regelungen für die Erledigung von Rechtshilfeersuchen. Nach Ziffer XII sind sich beide Seiten einig, dass der Spezialitätsgrundsatz einzuhalten ist. Zu den Ablehnungsgründen verweist Ziffer XIII auf das jeweilige nationale Recht. Auf der Grundlage von Ziffer XIII Abs. 1 Satz 3 kann auch eine im Einzelfall drohende unerträglich harte Strafe zur Ablehnung eines Ersuchens führen. Dies gilt insbesondere dann, wenn in Taiwan die Todesstrafe für die im Ersuchen beschriebene Tat droht. Zwar wird die Todesstrafe in Taiwan seit Jahren nur noch selten vollstreckt; eine Hinrichtung 2025[19] zeigt, dass in solchen Fällen stets eine ausdrückliche Zusicherung von taiwanesischer Seite einzuholen ist. Vorzusehen ist dabei auch eine Überprüfungsmöglichkeit für das Deutsche Institut Taipei. Zusicherungen sind nach Ziffer XV von der ersuchenden Seite abzugeben. Diese ist nach der Überschrift des Vertrages für Taiwan die Taipeh Vertretung in der Bundesrepublik Deutschland. Ziffer XII Abs. 2 und Ziffer XIV enthalten Konsultationspflichten vor Ablehnung eines Ersuchens. Die Datenschutzregelung unter Ziffer XVIII enthält nur einen Verweis auf das anzuwendende Recht beider Seiten. Soweit im Einzelfall Besonderheiten bestehen, kann darauf im Wege einer Bedingung hingewiesen werden.

Gemäß Ziffer XX ist die Absprache seit dem 11. Juni 2025 anwendbar, nachdem das Zustimmungsschreiben der taiwanesischen Stelle vom 28. Februar 2025 am 3. März 2025 und das Schreiben der deutschen Stelle vom 14. April 2025 am 12. Mai 2025 eingegangen ist.

V. Ausblick

Das Wirksamwerden der Absprache zur sonstigen Rechtshilfe zwischen der Bundesrepublik Deutschland und Taiwan verdeutlicht die Bereitschaft zur umfassenden Zusammenarbeit in Strafsachen. Die Absprache enthält Vereinbarungen zu Verfahrensvereinfachungen, die nach deutschem und taiwanesischem Recht keinen förmlichen Vertrag voraussetzen. Beide Seiten haben im Rahmen der Vertragsverhandlungen gezeigt, dass ein großes Interesse an einer vertrauensvollen und intensiven Kooperation besteht, damit die länderübergreifende Strafverfolgung durch gegenseitig geleistete Rechtshilfe gefördert werden kann. Inwieweit die Absprache sich bewähren wird, wird die Praxis zeigen.

Absprache

zwischen dem Deutschen Institut Taipei
und
der Taipeh Vertretung in der Bundesrepublik Deutschland
über die Zusammenarbeit auf dem Gebiet der justiziellen Rechtshilfe in Strafsachen

Das Deutsche Institut Taipei und
die Taipeh Vertretung in der Bundesrepublik Deutschland
(kurz: beide Seiten)
haben den Wunsch, im Bereich der Rechtshilfe zusammen zuarbeiten, und haben sich auf Folgendes verständigt:

I. Zweck

1. Beide Seiten beabsichtigen, in Übereinstimmung mit den Bedingungen ihrer jeweiligen Rechtsordnung auf dem Gebiet der Rechtshilfe in Strafsachen auf Ersuchen einander Unterstützung zu leisten. Diese Absprache soll nicht Ersuchen um die Auslieferung (oder die Festnahme oder Inhaftierung von Personen zum Zweck der Auslieferung), um die Vollstreckung strafrechtlicher Urteile der ersuchenden Seite auf der ersuchten Seite (mit Ausnahme von Urteilen betreffend Vermögensabschöpfung) sowie um die Überstellung von verurteilten Personen zur Verbüßung von Strafen erfassen.

2. Beide Seiten erklären sich deshalb bereit, auf der Grundlage der einschlägigen Gesetze und Vorschriften beider Seiten und nach den Grundsätzen der Menschlichkeit, Sicherheit, Zügigkeit, Einfachheit und Gegenseitigkeit Rechtshilfe zu leisten.

II. Begriffsbestimmungen

1. Die „ersuchende Seite“ bedeutet die Seite, die um Rechtshilfe bittet.

2. Die „ersuchte Seite“ bedeutet die Seite, die Rechtshilfe leisten soll.

III. Behörden

1. Die für die Umsetzung dieser Absprache zuständigen Kontaktbehörden werden sein:

a) das Deutsche Institut Taipei

b) die Taipeh Vertretung in der Bundesrepublik Deutschland

2. Die für die praktische Umsetzung dieser Absprache zuständigen Zentralen Behörden werden sein (im Folgenden: „Zentrale Behörden"):

a) die Abteilung für internationale und Cross-Strait-Rechtsangelegenheiten des Justizministeriums, Taiwan

b) das Bundesamt für Justiz

IV. Formelle Anforderungen an ein Ersuchen

1. Beide Seiten teilen die Auffassung, dass Rechtshilfeersuchen schriftlich gestellt und mit der Unterschrift der Kontaktbehörde der ersuchenden Seite versehen werden sowie einen bestimmten Inhalt aufweisen sollen, der gemäß der Rechtsordnung und Praxis der jeweiligen Seite insbesondere Folgendes einschließen sollte:

a) die Bezeichnung der zuständigen Behörde, welche das Strafverfahren, auf das sich das Ersuchen bezieht, führt;

b) soweit möglich, die Identität, die Staatsangehörigkeit oder vergleichbaren Status und den Aufenthaltsort der Person oder der Personen, gegen die sich das Strafverfahren richtet;

c) die Art der Strafsache, auf die sich das Ersuchen bezieht, sowie eine Zusammenfassung des Sachverhalts und eine Abschrift des anwendbaren Rechts;

d) den Zweck des Ersuchens und die Art der erbetenen Rechtshilfe;

e) gegebenenfalls Angaben über ein bestimmtes Verfahren oder Erfordernis, um dessen Einhaltung die ersuchende Seite bittet, und die Begründung dafür;

f) gegebenenfalls besondere Erfordernisse in Bezug auf die Vertraulichkeit (einschließlich des Schutzes personenbezogener Daten) und die Gründe dafür;

g) gegebenenfalls den Zeitraum, innerhalb dessen das Ersuchen erledigt werden soll;

h) alle sonstigen Angaben, die nötig sind, um die Erledigung des Ersuchens zu erleichtern;

i) bei Zustellungsersuchen die Identität und die Anschrift des Zustellungsempfängers sowie den Zusammenhang zwischen dieser Person und dem Verfahren;

j) bei Ersuchen um Abfrage, Durchsuchung, Sicherstellung oder Beschlagnahme die Tatsachen, die der Annahme zugrunde liegen, dass sich Beweismittel auf der ersuchten Seite befinden, die Umstände, die eine solche Maßnahme nach der Rechtsordnung der ersuchenden Seite rechtfertigen, sowie die Anordnung einer solchen Maßnahme durch eine zuständige Behörde oder eine Erklärung der Zentralen Behörde der ersuchenden Seite, aus der hervorgeht, dass eine solche Anordnung erwirkt werden könnte, wenn sich die Beweismittel auf der ersuchenden Seite befänden;

k) bei Ersuchen um Vernehmung einer Person deren Identität und Anschrift sowie den Gegenstand, zu dem die Person vernommen werden soll, einschließlich, soweit möglich, eines Fragenkatalogs sowie Angaben über das Bestehen eines Rechts des Betroffenen, die Aussage zu verweigern; wünscht die ersuchende Seite, dass Zeugen oder Sachverständige vor einem Richter, Staatsanwalt oder Polizeibeamten aussagen, so soll sie ausdrücklich darum ersuchen;

l) bei Ersuchen um Fahndung nach und Identifizierung von Personen Angaben zur Identität und, soweit möglich, zum Aufenthaltsort der Person, nach der gefahndet werden oder die identifiziert werden soll;

m) bei Ersuchen um Inaugenscheinnahme oder Untersuchung von Gegenständen eine Beschreibung des Gegenstands, von dem Augenschein eingenommen oder der untersucht werden soll;

n) bei der Überstellung einer in Haft befindlichen Person zur Beweiserhebung oder zur Unterstützung von Ermittlungen den Ort, an den die in Haft befindliche Person überstellt werden soll, und den geplanten Termin ihrer Rückkehr.

2. Beide Seiten teilen die Auffassung, dass Ersuchen und deren Anlagen bei Ersuchen des Deutschen Instituts Taipei eine Übersetzung ins traditionelle Chinesisch und bei Ersuchen der Taipeh Vertretung in der Bundesrepublik Deutschland eine Übersetzung in die deutsche Sprache beigefügt werden sollte.

V. Übermittlungswege

1. Ersuchen und Antworten darauf sollen gemäß der Rechtsordnung beider Seiten übermittelt werden.

2. Um das Verfahren zu beschleunigen, können Rechtshilfeersuchen zusätzlich vorab zwischen den Zentralen Behörden übermittelt werden, und zwar in schriftlicher und elektronischer Form.

3. Erforderlichenfalls können Anfragen betreffend Rechtshilfe in englischer Sprache unmittelbar zwischen den Zentralen Behörden gestellt werden.

VI. Arten der Rechtshilfe

1. Die Rechtshilfe unterliegt der Rechtsordnung der ersuchten Seite.

2. Rechtshilfemaßnahmen können alle Arten der Rechtshilfe einschließen, die der Rechtsordnung beider Seiten nicht zuwiderlaufen, insbesondere Folgendes:

a) Entgegennahme von Aussagen von Personen;

b) Vernehmung per Videokonferenz;

c) Überstellung inhaftierter Personen zu Aussage- oder sonstigen Zwecken;

d) Durchsuchung und Beschlagnahme;

e) Zustellung von Schriftstücken;

f) Überwachung von Telekommunikation, elektronischer Kommunikation und sonstiger Arten der Kommunikation;

g) Gemeinsame Ermittlungsgruppen;

h) Sicherstellung von Vermögenswerten;

i) Vollstreckung endgültiger und unwiderruflicher Urteile oder Anordnungen zur Einziehung von Vermögenswerten oder des Wertes von Erträgen im Zusammenhang mit einer Straftat;

j) Aufteilung von Vermögenswerten.

VII. Vernehmung per Videkonferenz

Für die Vernehmung per Videokonferenz sollen folgende Bestimmungen und Anforderungen Anwendung finden:

1. Bei der Vernehmung soll ein Vertreter einer Justizbehörde der ersuchten Seite, bei Bedarf unterstützt von einem Dolmetscher, anwesend sein, der auch die Identität der zu vernehmenden Person feststellen und auf die Einhaltung der Grundprinzipien der Rechtsordnung der ersuchten Seite achten soll;

2. die Vernehmung soll unmittelbar von oder unter Leitung der Justizbehörde der ersuchenden Seite gemäß deren Rechtsordnung durchgeführt werden;

3. auf Wunsch der ersuchenden Seite oder der zu vernehmenden Person soll die ersuchte Seite dafür sorgen, dass die zu vernehmende Person bei Bedarf von einem Dolmetscher unterstützt wird;

4. die zu vernehmende Person kann sich auf das Aussageverweigerungsrecht berufen, das ihr nach dem Recht der ersuchten oder der ersuchenden Seite zusteht.

VIII. Überstellung inhaftierter Personen

1. Eine auf der ersuchten Seite inhaftierte Person, deren Anwesenheit auf der ersuchenden Seite für die Zwecke der Rechtshilfe nach dieser Absprache erforderlich ist, kann aus der ersuchten Seite an die ersuchende Seite überstellt werden, wenn die Person einwilligt und wenn beide Seiten dem zustimmen.

2. Eine auf der ersuchenden Seite inhaftierte Person, deren Anwesenheit auf der ersuchten Seite für die Zwecke der Rechtshilfe nach dieser Absprache erforderlich ist, kann aus der ersuchenden Seite an die ersuchte Seite überstellt werden, wenn die Person einwilligt und wenn beide Seiten dem zustimmen.

3. Die Überstellung inhaftierter Personen unterliegt der jeweiligen Rechtsordnung beider Seiten. Dabei sollen sich die beiden Seiten an folgende Grundsätze halten:

a) Die übernehmende Seite soll befugt und verpflichtet sein, die überstellte Person in Haft zu halten, sofern die Behörden der überstellenden Seite nichts Anderes genehmigen;

b) die Behörden der übernehmenden Seite sollen die überstellte Person innerhalb eines angemessenen Zeitraums oder sobald die Umstände dies erlauben oder wie von beiden Seiten anderweitig vereinbart in die Haft der überstellenden Seite rücküberstellen;

c) die Behörden der übernehmenden Seite sollen von den Behörden der überstellenden Seite nicht verlangen, zur Rücküberstellung dieser Person ein Auslieferungsverfahren einzuleiten, und

d) der überstellten Person soll die in der übernehmenden Seite in Haft verbrachte Zeit auf die Verbüßung ihrer Strafe auf der überstellenden Seite angerechnet werden.

IX. Durchsuchung und Beschlagnahme

Die ersuchte Seite soll die Anwesenheit der in dem Ersuchen der ersuchenden Seite genannten Personen bei der Erledigung des Ersuchens zulassen.

X. Gemeinsame Ermittlungsgruppen

1. Beide Seiten können auf Grundlage ihrer jeweiligen Rechtsordnung und durch Absprache im Einzelfall eine gemeinsame Ermittlungsgruppe bilden. Ein von einer Seite entsandtes Mitglied einer gemeinsamen Ermittlungsgruppe kann mit der Durchführung von Ermittlungsmaßnahmen unter der Leitung des zuständigen Gruppenmitglieds der anderen Seite betraut werden, wenn die Rechtsordnungen beider Seiten es gestatten.

2. Die in einer gemeinsamen Ermittlungsgruppe tätigen Beamten können Beweismittel und Informationen, einschließlich personenbezogener Daten, die sie im Rahmen ihrer dienstlichen Aufgaben erlangt haben, unmittelbar an Mitglieder, die von einer Seite entsandt wurden, oder an andere Gruppenmitglieder weiterleiten, soweit dies für die Tätigkeit der gemeinsamen Ermittlungsgruppe erforderlich ist.

XI. Aufteilung von Vermögenswerten

Falls die von der ersuchten Seite geleistete Rechtshilfe zur erfolgreichen Einziehung von Vermögenswerten oder des Wertes von Erträgen durch die ersuchende Seite führt, können sich die beiden Seiten auf eine Aufteilung der Vermögenswerte nach ihrer jeweiligen Rechtsordnung einigen.

XII. Spezialität

Beide Seiten stimmen darin überein, dass eine Verwendung von Informationen oder Beweismitteln für andere Zwecke als die in dem Ersuchen genannten der vorherigen Zustimmung der Seite bedürfen soll, welche die be-

treffenden Informationen oder Beweismittel übermittelt, und dass die ersuchte Seite nach Konsultation der ersuchenden Seite verlangen können soll, dass überlassene Informationen oder Beweismittel oder deren Quelle vertraulich behandelt oder nur unter von ihr gestellten Bedingungen offenbart oder verwendet werden.

XIII. Ablehnungsgründe

1. Beide Seiten teilen die Auffassung, dass die ersuchte Seite nach ihrer Rechtsordnung die Erledigung eines Ersuchens ablehnen kann, insbesondere wenn die von der ersuchenden Seite erbetenen Maßnahmen der Rechtsordnung der ersuchten Seite zuwiderlaufen würden. Die ersuchte Seite soll ferner die Erledigung eines Ersuchens aufschieben können, wenn dies eine laufende Strafverfolgung auf der ersuchten Seite beeinträchtigen könnte. Beide Seiten betonen, dass ein Ersuchen abgelehnt werden kann, wenn davon ausgegangen wird, dass die Strafe für die vorgeworfene Straftat nach dem Recht der ersuchenden Seite den wesentlichen Wert der Menschenrechte, die Grundprinzipien des Rechts oder sonstige wichtige Belange der ersuchten Seite beeinträchtigt oder dagegen verstößt; im Falle Deutschlands gehören zu derartigen Belangen Verpflichtungen, die sich aus seiner Mitgliedschaft in der Europäischen Union und aus dem deutschen Grundgesetz ergeben.

2. Die ersuchte Seite kann eine als ausreichend erachtete Zusicherung, dass die vorgenannten wichtigen Belange nicht beeinträchtigt werden oder dass nicht gegen sie verstoßen wird, erbitten.

3. Weiterhin soll die ersuchte Seite die Erledigung eines Ersuchens ablehnen können, wenn diese die persönliche Sicherheit und andere legitime Rechte und Interessen einer an dem Verfahren beteiligten Person, eines Strafverfolgungsbeamten oder einer mit diesen verwandten oder in Verbindung stehenden Person gefährden würde.

4. Um die Ziele dieser Absprache bestmöglich zu verwirklichen, werden beide Seiten einander konsultieren, bevor die ersuchte Seite ein Ersuchen ablehnt oder die Erledigung eines Ersuchens aufschiebt, um zu prüfen, ob sie die begehrte Rechtshilfe unter bestimmten Bedingungen oder auf andere Weise leisten kann.

XIV. Erledigung von Ersuchen

1. Beide Seiten haben sich darauf verständigt, dass Ersuchen in Übereinstimmung mit der Rechtsordnung der ersuchten Seite umgehend und, soweit dieses Recht nicht entgegensteht, in der von der ersuchenden Seite erbetenen Weise erledigt werden sollen.

2. Beide Seiten teilen die Auffassung, dass die ersuchte Seite die ersuchende Seite umgehend von allen Umständen, die geeignet sind, die Erledigung des Ersuchens erheblich zu verzögern, und von ihrer Entscheidung, ein Rechtshilfeersuchen nicht oder nur teilweise zu erledigen oder die Erledigung aufzuschieben, unterrichten soll. Ist die ersuchte Seite der Ansicht, dass die zur Verfügung gestellten Informationen für die Erledigung des Ersuchens nicht ausreichen, so soll sie um ergänzende Informationen ersuchen, welche die Bearbeitung des Ersuchens ermöglichen. Die ersuchende Seite soll auf Ersuchen die ersuchte Seite über den Ausgang des Strafverfahrens unterrichten, auf das sich das Rechtshilfeersuchen bezieht.

3. Die ersuchte Seite soll die Anwesenheit der in dem Ersuchen der ersuchenden Seite genannten Personen bei der Erledigung des Ersuchens zulassen und diesen gestatten, der die Vernehmung/Befragung (der aussagenden Person) leitenden Person Fragen vorzuschlagen und sich Notizen zu machen, und zwar in einer Weise, der die ersuchte Seite zugestimmt hat.

XV. Zusicherungen

1. Gibt die ersuchende Seite eine Zusicherung ab, so wird vorbehaltlich ihrer Rechtsordnung und dieser Absprache von ihr die Einhaltung dieser Zusicherung erwartet. Knüpft die ersuchte Seite die Rechtshilfe an eine Bedingung und nimmt die ersuchende Seite die Rechtshilfe an, so wird von der ersuchenden Seite die Einhaltung dieser Bedingung erwartet, soweit dies mit ihrer Rechtsordnung und mit dieser Absprache vereinbar ist.

2. Hat die ersuchende Seite Zusicherungen abgegeben oder wird von ihr die Einhaltung einer Bedingung erwartet, so wird die ersuchende Seite eine wirksame Überprüfung der Einhaltung der Zusicherungen oder Bedingungen gewähren oder spezifische Informationen zur Verfügung stellen.

XVI. Vertraulichkeit

Die ersuchende Seite kann von der ersuchten Seite verlangen, das Ersuchen und seinen Inhalt vertraulich zu behandeln, soweit dies mit der Erledigung des Ersuchens vereinbar ist. Kann die ersuchte Seite die Vertraulichkeit nicht wahren, wird sie unverzüglich die ersuchende Seite darüber unterrichten.

XVII. Konsultationen

1. Die Zentralen Behörden sollen einander zu gemeinsam vereinbarten Zeitpunkten konsultieren, um eine möglichst wirksame Zusammenarbeit in den von dieser Absprache erfassten Bereichen zu fördern und bessere praktische Maßnahmen zur Erleichterung dieser Zusammenarbeit zu entwickeln.

2. Um die Durchführung dieser Absprache zu erleichtern, können beide Seiten anbieten, Rechtsmaterialien (z. B. die Grundsätze des Schutzes personenbezogener Daten) als Referenz zur Verfügung zu stellen.

XVIII. Schutz personenbezogener Daten

Die Verarbeitung personenbezogener Daten in den von dieser Absprache erfassten Fällen müsste unter vollstän-

diger Einhaltung des anwendbaren Rechtsrahmens beider Seiten, einschließlich der EU-Rechtsvorschriften zum Datenschutz, erfolgen.

XIX. Kosten

Beide Seiten teilen die Auffassung, dass die mit der Erledigung des Ersuchens verbundenen Kosten gemäß den anwendbaren Vorschriften ihrer Rechtsordnung die ersuchte Seite tragen soll. Stellt sich heraus, dass die Erledigung des Ersuchens mit außergewöhnlichen Kosten verbunden ist, so sind sich beide Seiten darüber einig, dass sie, vorzugsweise vor Erledigung des Ersuchens, eine abweichende Kostenverteilung erörtern können. Dies soll insbesondere möglich sein bei

1. Kosten, die mit der Beförderung einer Person in das oder aus dem Gebiet der ersuchten Seite auf Ersuchen der ersuchenden Seite verbunden sind, einschließlich der Kosten für den erforderlichen Einsatz von Begleitpersonal, sowie die Entschädigung oder die Kosten, die dieser Person im Zusammenhang mit der Erledigung des Ersuchens zu erstatten sind;
2. Kosten und Honoraren von Sachverständigen;
3. Übersetzungs-, Dolmetscher- und Transkriptionskosten;
4. Kosten, die mit der Beweiserhebung auf der ersuchenden Seite über eine Videoschaltung aus der ersuchten Seite verbunden sind;
5. Kosten, die mit der Verwaltung von Vermögenswerten verbunden sind.

XX. Schlussbestimmungen

1. Beide Seiten werden die nach dieser Absprache vorgesehene Zusammenarbeit am dreißigsten Tag beginnen, nachdem beide Seiten einander schriftlich informiert haben, dass sie bereit sind, diese Zusammenarbeit aufzunehmen. Diese Absprache soll am Tag der späteren dieser beiden Benachrichtigungen wirksam werden.
2. Diese Absprache wird in zwei Exemplaren, jeweils in chinesischer, deutscher und englischer Sprache, unterzeichnet, wobei alle Sprachfassungen gleichwertig sind.
3. Bei unterschiedlicher Auslegung des chinesischen und des deutschen Wortlauts kann der englische Wortlaut als Auslegungshilfe dienen.

Dr. Ralf Riegel
Ehem. Leiter des Referats für Internationales Strafrecht im Bundesministerium der Justiz

Teresa Steiger
Oberstaatsanwältin, Staatsanwaltschaft Siegen

* Die Ausführungen in diesem Artikel stellen die persönliche Auffassung der Autoren dar.

1 Deutsches Institut Taipei, *Taiwan: Politisches Portrait*, Stand 22.10.2025, <https://taipei.diplo.de/tw-de/aktuelles-in-taiwan/laenderinformationen/innenpolitik>. Alle Hyperlinks in diesem Artikel wurden zuletzt aufgerufen am 28.03.2026.

2 Resolution 2758, "Restoration of the lawful rights of the People's Republic of China in the United Nations, abrufbar unter: <https://digitallibrary.un.org/record/192054?v=pdf>. Siehe zum Diskurs auch <https://digitallibrary.un.org/record/735611?v=pdf>.

3 Vgl. nur die Präambel der Verfassung der Volksrepublik China, <https://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e9499913.html>.

4 Vgl. zum Beispiel die Entschließung des Europäischen Parlaments vom 24. Oktober 2024 zu der falschen Auslegung der UN-Resolution 2758 durch die Volksrepublik China und ihren ständigen militärischen Provokationen rund um Taiwan (2024/2891(RSP) und den "Taiwan International Solidarity Act" des Ausschusses für auswärtige Angelegenheiten des United States House Committee on Foreign Affairs aus dem Jahr 2023, <https://www.govinfo.gov/app/details/BILLS-118hr1176ih>.

5 Information des taiwanesischen Außenministeriums, <https://en.mofa.gov.tw/AlliesIndex.aspx?n=1294&sms=1007>.

6 Information des deutschen Auswärtigen Amtes, *Deutschland und China: Bilaterale Beziehungen*, Stand: 04.07.2023, <https://china.diplo.de/cn-de/willkommen-in-china/politik/bilateral-2593306> und *Deutschland und Taiwan: Bilaterale Beziehungen,* Stand 22.10.2025, <https://www.auswaertiges-amt.de/de/service/laender/taiwan-node/bilateral-200904>.

7 G. Jellinek, *Allgemeine Staatslehre*, 3. Auflage 1914, S. 396 ff; dazu erläuternd V. Epping, in: Knut Ipsen, *Völkerrecht*, 7. Auflage 2018, S. 76 ff.

8 Epping a.a.O., S. 76, 155 ff m.w.N.

9 A. Heidemann-Grüder, „Analyse: Postsowjetische De-facto-Regime", *Bundeszentrale für politische Bildung (bpb)*, 01.12.2020, <https://www.bpb.de/themen/europa/russland-analysen/nr-394/322085/analyse-postsowjetische-de-facto-regime/>; M. Herdegen, *Völkerrecht*, 22. Auflage 2023, § 11 Rdnr. 1.

10 G. Gornig, *Völkerrecht*, 2023, § 20 Rn. 5 ff; David X. Noack, „De-facto-Staaten – Prekäre Staatlichkeit und eingefrorene Konflikte", *W&F Wissenschaft und Frieden* 4/2017, <https://wissenschaft-und-frieden.de/artikel/de-facto-staaten/#:~:text=Probleme%20stabilisierter%20De-facto-Regime,Schwebezustand%20durch%20Gewalt%20zu%20l%C3%B6sen> .

11 Gornig, *op. cit.* (n. 10).

12 J. Abr. Frowein, „Der völkerrechtliche Status Taiwans und seine

Rolle als begrenztes Völkerrechtssubjekt", DOCPLAYER, <https://docplayer.org/56960397-Der-voelkerrechtliche-status-taiwans-und-seine-rolle-als-begrenztes-voelkerrechtssubjekt-prof-dr-dres-h-c-jochen-abr-frowein.html>; M. Neukirchen, „Taiwan: eigenständig, aber nicht souverän", *Vereinte Nationen* 2/2005, 50 ff., <https://zeitschrift-vereinte-nationen.de/publications/PDFs/Zeitschrift_VN/VN_2005/Heft_2_2005/Beirag_Neukirchen_VN_2_05.pdf>; Wissenschaftliche Dienste des Deutschen Bundestags, „Völkerrechtliche Aspekte eines potentiellen bewaffneten Konflikts zwischen der Volksrepublik China und Taiwan", <https://www.bundestag.de/resource/blob/938168/b0f334e6c4cb428134df8c069e2e3d0c/WD-2-012-23-pdf-data.pdf>, S. 5; anders Herdegen, *op. cit.* (n. 9): „ staatsähnlicher Herrschaftsverband eigener Art".

13 Für die Auslieferung siehe § 2 Abs. 1 und 2 IRG, für Durchlieferung siehe § 43 Abs. 1 IRG, für die sonstige („kleine") Rechtshilfe siehe § 59 Abs. 1 IRG, für die Vollstreckungshilfe siehe §§ 48, 56b IRG, für die Datenübermittlung ohne Ersuchen siehe § 61a IRG.

14 OLG Frankfurt, Beschluss vom 26. August 2022, 2 AuslA 168/22; eine Durchlieferung an Taiwan wurde mit Beschluss vom 10. Januar 2024, 2 AuslD 4/24 ermöglicht, da der ausliefernde Staat die Fragen geprüft habe und dessen Entscheidung insoweit verbindlich sei.

15 Auslieferungs-Vertrag zwischen dem Deutschen Reiche und Großbritannien. Deutsches Reichsgesetzblatt Band 1872, Nr. 21, Seite 229 – 237, <https://de.wikisource.org/wiki/Auslieferungs-Vertrag_zwischen_dem_Deutschen_Reiche_und_Gro%C3%9Fbritannien> .

16 W. Appel, *Internationale Rechtshilfe in Strafsachen ohne diplomatischen Geschäftsweg*, 2017, Seite 105 f; R. Riegel/F. Fülle, "Vollstreckungshilfe zwischen Deutschland und Taiwan auf neuer Grundlage", (2016) *eucrim*, 61; R. Riegel, in: Schomburg/Lagodny, *Internationale Rechtshilfe in Strafsachen*, 6. Auflage 2020, § 1 IRG, Rn. 7.

17 Der Act is abrufbar unter: <https://mojlaw.moj.gov.tw/ENG/LawContentE.aspx?LSID=FL088318>.

18 Dazu Riegel/Fülle, (2016) *eucrim, op. cit.* (n. 16), 61–64.

19 Amnesty International, „Taiwan: Erste Hinrichtung seit 2020 – ein beschämender Rückschlag", 18.01.2025, <https://amnesty-todesstrafe.de/2025/01/taiwan-erste-hinrichtung-seit-2020-ein-beschaemender-rueckschlag/>; Szu-Yu (Suzy) Chen, „The Death Penalty in Taiwan: An Overview and the Impact of 113-Hsien-Pan-8", *University of Nottingham – Taiwan Research Hub*, 14.03.2025, <https://taiwaninsight.org/2025/03/14/the-death-penalty-in-taiwan-an-overview-and-the-impact-of-113-hsien-pan-8/>.

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. 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; Prof. Dr. Esther Herlin-Karnell, University of Gothenburg, Sweden; Dr. Fabio Giuffrida, Head of Section (Antifraud Criminal Policy), DG Justice and Consumers, European Commission; 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, Former Head of Unit, European Commission (Anti-Fraud Office (OLAF) and Directorate for Audit in Cohesion (DAC)); 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 (ret.), Italy; Prof. Rosaria Sicurella, University of Catania, Italy
Language Consultants: Indira Tie and Sarah Norman, Certified Translators, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Typeset and Layout: Ines Hofmann and 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)
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. Articles can be published in English, French and German.
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