

# eucrim

2024 /

# 3

European Law Forum: Prevention • Investigation • Prosecution



## Digitalisation of Justice

La numérisation de la justice

Digitalisierung der Justiz

Guest Editorial by *Jorge Espina*

*Ioana Mazilescu and Katerina Entcheva*: Artificial Intelligence and Digitalisation of Judicial Cooperation – The Main Provisions in Recent EU Legislation

*Georg Roebing and Bogdan Necula*: Reflections on Introducing Artificial Intelligence Tools in Support of Anti-Fraud

*Boudewijn de Jonge and Barry de Vries*: Data-Driven Investigations in a Cross-Border Setting – Experiences from the Netherlands

*Lorena Bachmaier Winter*: A Plea for Common Standards on the Lawyer- Client Privilege in EU Cross-Border Criminal Proceedings in Light of Advancing Digitalisation

*Tomohiro Nakane*: Enhancing the Right of Access to a Lawyer for Detained Suspects and Accused Persons via Videoconferencing – The Situation in Germany and Proposals for Improvement

*Judit Szabó and Dominik Brodowski*: Transnational Virtual Criminal Trials in the European Union – Reflections on Occasion of Joined Cases C-255/23 (AVVA and Others) and C-285/23 (Linte) at the CJEU

*Randall Stephenson and Johanna Rinceanu*: Differential Diagnosis in Online Regulation – Reframing Canada's "Systems-Based" Approach

euocrim 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://euocrim.eu/associations/>.

## Contents

### News

#### European Union

##### Foundations

- 174 Area of Freedom, Security and Justice
- 174 Ukraine Conflict
- 176 Artificial Intelligence (AI)
- 178 Digital Space Regulation

##### Institutions

- 179 European Court of Justice (ECJ)
- 180 European Public Prosecutor's Office (EPPO)
- 182 Europol
- 182 Eurojust
- 183 European Judicial Network (EJN)
- 183 Frontex

##### Specific Areas of Crime

- 184 Protection of Financial Interests
- 186 Tax Evasion
- 188 Counterfeiting & Piracy

##### Procedural Law

- 189 Data Protection
- 192 Victim Protection

##### Cooperation

- 193 European Arrest Warrant
- 193 Law Enforcement Cooperation

#### Council of Europe

##### Foundations

- 194 Artificial Intelligence (AI)
- 197 Human Rights Issues

##### Institutions 197

- 197 European Committee on Crime Problems (CDPC)

##### Specific Areas of Crime 197

- 197 Corruption
- 198 Money Laundering

##### Procedural Law 199

- 199 European Commission for the efficiency of justice (CEPEJ)
- 200 Consultative Council of European Public Prosecutors (CCPE)

### Articles

#### Digitalisation of Justice

- 201 Fil rouge  
*Thomas Wahl*
- 202 Artificial Intelligence and Digitalisation of Judicial Cooperation – The Main Provisions in Recent EU Legislation  
*Ioana Mazilescu and Katerina Entcheva*
- 206 Reflections on Introducing Artificial Intelligence Tools in Support of Anti-Fraud  
*Georg Roebeling and Bogdan Necula*
- 214 Data-Driven Investigations in a Cross-Border Setting – Experiences from the Netherlands  
*Boudewijn de Jonge and Barry de Vries*
- 222 A Plea for Common Standards on the Lawyer-Client Privilege in EU Cross-Border Criminal Proceedings in Light of Advancing Digitalisation  
*Lorena Bachmaier Winter*
- 230 Enhancing the Right of Access to a Lawyer for Detained Suspects and Accused Persons via Videoconferencing – The Situation in Germany and Proposals for Improvement  
*Tomohiro Nakane*
- 237 Transnational Virtual Criminal Trials in the European Union – Reflections on Occasion of Joined Cases C-255/23 (AVVA and Others) and C-285/23 (Linte) at the CJEU  
*Judit Szabó and Dominik Brodowski*
- 245 Differential Diagnosis in Online Regulation – Reframing Canada's "Systems-Based" Approach  
*Randall Stephenson and Johanna Rinceanu*

# Guest Editorial

Dear Readers,

Digitalisation is not just the future but already an undeniable reality in today's society! Our task now is to strive for its best and most efficient use. For actors involved in international cooperation, in particular, digitalisation involves a number of sweeping technical and legal changes as well as changes to our mind-set. In the words of American writer *Stewart Brand*, "Once a new technology rolls over you, if you're not part of the steamroller, you're part of the road."

Several commendable digitalisation reforms have been set in motion, including in the field of criminal law. The widely welcomed Regulation (EU) 2023/2844 on Digitalisation of Judicial Cooperation introduces the digital transformation of the justice sector. Its provisions on videoconferencing and the transmission of mutual recognition requests via a decentralised IT system are perfect examples of the open-minded response to this challenging and unstoppable trend. The impact of the Digitalisation of Judicial Cooperation Committee is visible: it brings together the relevant services and authorities from EU Member States and EU bodies/agencies to discuss the necessary introduction of changes to the various cooperation instruments.

In addition, Joint Investigation Teams (JITs) are being adapted to the digital environment. One reform that will soon take root is the new Collaboration Platform (established by Regulation (EU) 2023/969). It will allow JIT members to access a digital platform where all evidence in electronic format will be at the disposal of the national authorities involved and available for the relevant national criminal proceedings. Existing tools have been upgraded to transition to the digital age and practitioners staffed with the adequate resources.

The new EU legislation on e-evidence (Regulation (EU) 2023/1543 and Directive (EU) 2023/1544) represents perhaps the most significant and certainly challenging step forward. It marks a revolution in the mutual recognition instruments: for the first time, a cooperation instrument does not connect two competent authorities of different Member States, but now one judicial authority interacts with a representative of a private entity; depending on the circumstances, the entire process of executing a request may take place without any involvement of a public authority in the

executing Member State (the enforcing authority).

The Digital Services Act (Regulation (EU) 2022/2065) has also gained relevance. It aims to protect the digital space against the spread of illegal content while at the same time ensuring the protection of fundamental rights by creating a safe and trusted online environment for users. In contrast to the initiatives mentioned above, the Act does not focus on public authorities and their ways of cooperation. It is a necessary complement that provides the private sector with a common ground from which it can work together with the public sector.

The EU is also pioneering legislation in the field of Artificial Intelligence (AI) with the recent AI Act (Regulation (EU) 2024/1689). It tackles crucial issues, e.g., the definition of prohibited or high-risk AI systems, and includes obligations for providers and deployers. The possibility to use real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is a complex topic that is also under consideration by the Union legislature.

We, as practitioners, must reflect on these digital challenges and swiftly bring the new legal mechanisms into operation. The actors involved (including EU agencies such as Eurojust and Europol, networks like the European Judicial Network and the European Judicial Cybercrime Network, and private entities) are working hard towards cooperation, so that all these innovative instruments become a coherent, efficient, and synchronised machinery, able to produce the necessary results for the well-being of our society.

Let's contribute to change our mindsets towards the new digital future!

**Jorge Espina**

Prosecutor, Deputy National Member for Spain at Eurojust, EJM contact point



Jorge Espina



### European Union

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

#### Foundations

##### Area of Freedom, Security and Justice

##### ECJ Ruled on Res Judicata Effects of Administrative Court Decision before Criminal Courts

On 26 September 2024, the Court of Justice of the European Union (ECJ) issued a judgment in [Case C-792/22](#) (“*Energotehnica*”) addressing the binding force of administrative court judgments for criminal proceedings and the primacy of EU law over conflicting national court decisions. The case arose from the death of an electrician who was fatally electrocuted at work. The incident raised questions about employer responsibility under [Directive 89/391/EEC](#), which requires employers to ensure worker safety, and about the compatibility of Romanian procedural rules with EU law.

Under Romanian law, as interpreted by the Romanian Constitutional Court, administrative court decisions are binding on criminal courts (*res judicata*). Since, in the case at issue, the administrative court concluded that there was no “accident at work” and annulled the

administrative penalties imposed on the employer, the criminal court, before which criminal proceedings for negligence and manslaughter took place in parallel, was prevented from reconsidering whether the accident constituted an accident at work. The referring Court of Appeal, Braşov (Romania), doubted whether the Romanian legal situation, where administrative court decisions have a strong force of *res judicata* before the criminal court and which effectively excludes the successors of a victim being heard in any of the proceedings deciding on liability, is compatible with EU law.

The ECJ ruled that such legislation is incompatible with EU law if it denies the successors of the victim the right to be heard in any of the proceedings determining whether the incident constitutes an accident at work. This contravenes the principle of effectiveness under EU law and the right to an effective remedy enshrined in Art. 47 of the Charter of Fundamental Rights of the European Union.

Furthermore, the Court addressed the broader issue of EU law primacy. It ruled that the principle of EU law precludes national legislation or practices

that prevent ordinary courts from disapplying decisions of a national constitutional court that conflict with EU law. Specifically, it held that judges must not be subject to disciplinary proceedings for refusing to apply national constitutional court rulings when they infringe EU rights, such as those under Directive 89/391. National judges must retain the independence to ensure the full application of EU law, even if this requires setting aside conflicting rulings by higher national courts.

The judgment in *Energotehnica* reinforces the importance of ensuring effective remedies for violations of EU law, particularly in the context of worker safety. It bans an absolute *res judicata* effect of administrative court decision over criminal proceedings. The ECJ required that fundamental rights, such as the right to be heard under Art. 47 of the Charter, must be taken into account.

The ECJ’s judgment also underscores the primacy of EU law over national legal systems. It affirms the employer’s duty to provide safe working conditions and protects the right of individuals to access justice when these obligations are not met. It safeguards judicial independence by affirming that national courts must have the authority to prioritize EU law in cases of conflict. (AP)

#### Ukraine Conflict

##### EU Reactions to Russian War against Ukraine: Overview October – November 2024

This news item continues the reporting on key EU reactions following the Russian invasion of Ukraine on 24 February 2022: the impact on the EU’s in-

\* Unless stated otherwise, the news items in the following sections cover the period 16 September 2024 – 15 November 2024. Have a look at the eucrim website (<https://eucrim.eu>), too, where all news items have been published beforehand.

ternal security policy, on criminal law, and on the protection of the EU's financial interests. The following overview covers the period from October 2024 to November 2024. For overviews of the previous developments: from February 2022 to mid-July 2022 → [eucrim 2/2022, 74–80](#); from the end of July 2022 to the end of October 2022 → [eucrim 3/2022, 170–171](#); from November 2022 to December 2022 → [eucrim 4/2022, 226–228](#); from January 2023 to June 2023 → [eucrim 1/2023, 6–9](#); from July 2023 to September 2023 → [eucrim 2/2023, 116–117](#); from October 2023 to January 2024 → [eucrim 4/2023, 313–315](#); from January 2024 to June 2024 → [eucrim 1/2024, 9–11](#); from July 2024 to September 2024 → [eucrim 2/2024, 94–95](#).

- 8 October 2024: In response to Russia's hybrid actions towards the EU, the Council adopts a new legal framework of restrictive measures to target individuals and entities responsible for supporting or benefiting from Russia's destabilizing activities globally. [Council Decision \(CFSP\) 2024/2643](#) introduces new grounds on the basis of which the EU can impose smart sanctions against natural or legal persons who are involved in Russia's hybrid campaigns. Importantly, the new legal regime not only applies to activities directed against the EU and its Member States, but also to Russian hybrid activities targeting international institutions or third countries.
- 8 October 2024: In a [statement by the High Representative](#) for Foreign Affairs and Security Policy accompanying the Council Decision concerning restrictive measures in view of Russia's destabilizing activities, the European Union strongly condemn Russia's escalating hybrid actions against the EU, its Member States, and partners. According to the statement, the alleged behaviour can be deemed reckless, irresponsible, and in violation of international law and the rules-based international order. These activities include cyber-attacks, disinformation campaigns, sabotage,

arson, and the instrumentalisation of migration, as well as disruptions to satellite communications, violations of European airspace, and physical attacks on individuals within the EU. The EU identifies these actions as part of a coordinated hybrid campaign by Russia aimed at dividing European society, destabilising Member States, weakening resilience, and undermining EU support for Ukraine.

- 11 October 2024: At the [JHA Council meeting](#), the Hungarian Council Presidency, the Commission and Euro-just give an update on the most recent developments as regards the fight against impunity of war crimes committed in the context of Russia's war of aggression against Ukraine. Ministers welcome that Ukraine adopted legislation on 24 August 2024 to pave the way for Ukraine's accession to the Rome Statute.

- 11 October 2024: A [new factsheet](#) provides information on the key achievements of the von der Leyen Commission in supporting Ukraine against Russia's war of aggression. The factsheet mentions, for instance, that, since the beginning of the war, the EU has mobilised and developed unique means of economic, humanitarian, and military assistance, bringing the total support provided by the EU and its Member States to almost €124 billion, including €1.5 billion from the proceeds of Russian immobilised assets. The factsheet also highlights the Ukraine Facility, which will provide Ukraine with up to €50 billion in the form of grants and concessional loans between 2024 and 2027.

- 14 October 2024: The Council [adopts restrictive measures](#) against five individuals and a Russia-based non-governmental association whose goal is to promote Russia's interests abroad. They are held responsible for destabilising actions in Gagauzia, an autonomous territorial unit in Moldova. The sanctions impose asset freezes, travel bans within the EU, and prohibit

providing funds or economic resources to the listed individuals and entity. These measures increase the total under the EU's sanctions framework for Moldova to 16 individuals and two entities. This sanctions framework, established in April 2023, addresses actions that undermine Moldova's sovereignty, democracy, and security. Destabilisation efforts, which have intensified with Russia's aggression against Ukraine, directly threaten the stability of the EU's external borders.

- 14 October 2024: The Council [adopts](#) restrictive measures against seven individuals and seven entities in [response to Iran's transfers of missiles and drones to Russia](#) for use in its war against Ukraine. These measures follow the European Council's March 2024 warning of swift action if Iran were to transfer ballistic missiles or related technology to Russia. The sanctions target individuals and entities involved in developing and transferring unmanned aerial vehicles (UAVs), missiles, and related technology.

- 17 October 2024: The [European Council takes several conclusions on Ukraine](#). The European Council reaffirms its unwavering support for Ukraine in the face of Russia's continued aggression, condemns the violations of international law and pledges comprehensive assistance across political, financial, military, and humanitarian domains. It emphasises the importance of a just and lasting peace based on the UN Charter and Ukraine's Peace Formula, while asserting that no decisions about Ukraine will be made without its involvement. The G7 commitment of €45 billion to support Ukraine's military, budgetary, and reconstruction needs is reiterated and the use of extraordinary revenues from immobilised Russian assets to aid Ukraine, subject to legal safeguards, is highlighted. The conclusions also back Ukraine's recovery and reconstruction efforts and support displaced persons, including refugees



in EU countries, by ensuring adequate financial assistance to Member States carrying the largest burdens. Lastly, the European Council reiterates its commitment to Ukraine's integration into the European Union, emphasising continued reform support on its path toward EU membership.

■ 24 October 2024: On behalf of the EU, the High Representative for Foreign Affairs and Security Policy [expresses](#) deep alarm over reports that the Democratic People's Republic of Korea (DPRK) is sending troops to support Russia's illegal war of aggression against Ukraine. The EU also criticises Russia's concerning shift on denuclearisation, accusing it of violating its obligations under the Non-Proliferation Treaty (NPT) and compromising its responsibilities as a permanent UN Security Council member. It reiterates that the DPRK cannot achieve nuclear weapon state status under the NPT.

■ 29 October 2024: [Regulation \(EU\) 2024/2773 of the European Parliament and of the Council](#) enters into force which establishes the Ukraine Loan Cooperation Mechanism and makes available to Ukraine exceptional macro-financial assistance in the form of a loan (the "MFA Loan") with a view to supporting Ukraine in covering its urgent financing needs arising from Russia's ongoing aggression. The mechanism supports Ukraine in repaying up to €45 billion in loans provided by the EU and G7 partners. The repayment of these loans relies on future revenues generated from immobilised Russian sovereign assets, alongside voluntary contributions from EU Member States, third countries, and other sources. The MFA loan is linked to policy conditions under the Ukraine Facility and Ukraine Plan, with oversight systems in place to prevent fraud and irregularities.

■ 30 October 2024: The European Commission adopts its [2024 Enlargement Package](#), highlighting significant progress made by Ukraine on its path toward EU accession. The opening

of accession negotiations in June 2024 marked a milestone, recognising Ukraine's commitment to pursuing critical reforms despite the challenges posed by Russia's ongoing aggression. The screening process, a key step in aligning Ukrainian law with EU standards, is progressing smoothly. The Commission anticipates the opening of negotiations on policy clusters, starting with the fundamentals, as early as 2025, provided Ukraine meets the necessary conditions.

■ 8 November 2024: The Council adopts a [decision extending the mandate of the European Union Military Assistance Mission](#) in support of Ukraine (EUMAM Ukraine) by two more years, until 15 November 2026, with a budget allocation of nearly €409 million for the period from November 2024 to 2026. EUMAM Ukraine remains central to the EU's military support, focusing on enhancing the military capacity of Ukraine's Armed Forces (UAF). Under the extended mandate, EUMAM Ukraine will cooperate with NATO, particularly through the NATO Security Assistance and Training for Ukraine (NSATU), ensuring transparent and reciprocal information sharing.

■ 14 November 2024: The Commission [gives a positive statement](#) that Ukraine has satisfactorily fulfilled the nine agreed reform indicators for a further payment of over €4 million under the Ukraine Facility. Accomplished steps for the payment include increased capacity building to fight corruption in Ukraine and measures for improved asset recovery. For the disbursement of the money, the Council must confirm the Commission's conclusions and adopt an implementing decision.

■ 18 November 2024: The [Council broadens the scope of restrictive measures against Iran](#) due to its military support for Russia's war in Ukraine and armed groups in the Middle East and Red Sea regions. The new legal

framework allows the EU to target the use of vessels and ports for transferring Iranian-made drones (UAVs), missiles, and related components. The EU introduces a ban on exporting, transferring, and supplying components from the EU to Iran that are used for missile and UAV production. A transaction ban is also imposed, prohibiting dealings with ports and locks owned, operated, or used for transferring Iranian UAVs, missiles, or related technology to Russia. [Additionally, the Council sanctions](#) one individual and four entities following Iran's missile and drone transfers to Russia. (AP/TW)

## [Artificial Intelligence \(AI\)](#)

### [Europol Report: Benefits and Challenges of AI for Law Enforcement](#)

**spot light** For the first time, Europol's Innovation Lab has published an [Observatory Report on AI and Policing](#), which aims to provide an overview of the benefits and challenges associated with the adoption of artificial intelligence (AI) by law enforcement. The report seeks to show how the rapidly evolving AI technology can contribute to enhancing the efficiency, effectiveness, and overall performance of law enforcement operations, while upholding ethical and legal standards. It is primarily aimed at Law Enforcement Agencies (LEA) operating across the EU but should also be of value to other readers, such as policymakers, technology developers, academics, civil rights advocates, and the general public, both within the EU and globally.

The report looks at applications of AI in law enforcement, such as data analytics, digital forensics, computer vision, and biometrics, and generative AI. It goes on to analyse technological limitations and challenges as well as ethical and social issues in AI for law enforcement, for example data bias and fairness, privacy and surveillance, accountability and transparency, and

human rights and discrimination. It also provides an overview of the objectives, scope, and key provisions of the EU Artificial Intelligence Act and its implications for law enforcement agencies. The report concludes with an outlook and a set of key takeaways, including:

- The potential of AI to significantly transform policing – from advanced criminal analytics that reveal trends in vast amounts of data, to biometrics that allow the prompt and unique identification of criminals;
- The ability to integrate large and complex datasets and natural language processing into policing applications allows for the extraction of actionable insights, and improves resource forecasting and operational efficiency, while these technologies can simultaneously protect and uphold privacy rights;
- AI-driven tools, including in the context of OSINT and SOCMINT, that can process unstructured data to provide real-time insights are improving the ability of law enforcement to more effectively and efficiently address urgent situations such as crimes against children and terrorism;
- Technologies like machine translation are crucial to facilitate international collaboration among law enforcement agencies;
- The fusion of AI and biometrics can enhance criminal identification accuracy while protecting the privacy of non-relevant individuals;
- Generative AI represents the next leap, from passive analysis to active creation, and offers many opportunities for law enforcement. But as with any tool, its power lies in its judicious and ethical use, balancing innovation with responsibility;
- Substantial technological infrastructure and expertise is required to effectively develop and deploy AI technologies, which presents significant challenges, particularly for smaller law enforcement agencies;

- To ensure appropriate data handling and responsible data processing practices, law enforcement agencies must invest in training and raising awareness amongst their staff to navigate these complex legal and ethical landscapes;

- Compliance with the EU AI Act represents a crucial balancing act, as it requires law enforcement to adhere to stringent ethical, legal, and privacy standards, potentially necessitating the reassessment of existing AI tools;

- The EU AI Act challenges law enforcement agencies to allocate additional resources and navigate the complexities of compliance. This is especially relevant for those agencies developing AI tools in house, emphasising the need for a responsible and ethical approach to AI integration in law enforcement;

- Police forces, which may already be utilising certain AI systems, will face the challenging task of re-evaluating these tools. Should any of these operational technologies fall within the prohibited category set by the EU AI Act, they would need to be deactivated, leading to potential challenges in maintaining operational continuity;

- Addressing bias in AI is paramount, with a need for systems that are not only technically sound but also embody fairness, justice, and impartiality, ensuring that data collection and storage adhere to strict privacy guidelines;

- Accountability, transparency, and explainability are essential, not only for ethical and responsible AI use but also to ensure that evidence collected and analysed by AI systems withstands scrutiny, respect the right to a fair trial, and is deemed acceptable in court proceedings;

- Regular audits of AI systems are essential to ensuring compliance with established privacy and data protection standards, maintaining a balance between harnessing AI-driven insights and safeguarding fundamental rights and individual freedoms.

Looking to the future, quantum computing, 6G connectivity, automated drones and robotics, AI chips, and edge computing are on the verge of opening up new possibilities for law enforcement, if used ethically and in accordance with the principles of justice and fairness. Public trust and acceptance are seen as cornerstones for the successful integration of AI technologies into law enforcement. The report therefore emphasises the need to invest in community engagement, education, and feedback mechanisms. Lastly, strengthening collaboration and knowledge sharing in the form of inter-agency cooperation, partnerships with academia and industry, and engagement with civil society, among others, is seen as essential to the success of integrating AI into law enforcement. (CR) ■

#### Over 100 Companies Commit to EU AI Pact

On 25 September 2024, the European Commission announced that over 100 companies have signed the EU Artificial Intelligence (AI) Pact, committing to voluntary pledges to promote trustworthy and safe AI development ahead of the AI Act's full application. The [signatories include](#) multinational corporations and European SMEs across sectors like IT, healthcare, banking, and automotive.

The pact requires companies to focus on three main areas:

- Developing an AI governance strategy for future AI Act compliance;
- Identifying high-risk AI systems;
- Promoting AI literacy and ethical practices among staff.

Over half of the companies also pledged additional commitments, such as ensuring human oversight, mitigating risks, and transparently labeling AI-generated content such as deepfakes.

In parallel, the Commission has [launched initiatives](#) to strengthen EU leadership in AI innovation, including the AI Factories initiative to support

start-ups and industries with resources like data and computing power. The initiative aims to advance AI applications in critical sectors such as healthcare, energy, and aerospace. Additional measures include venture capital support, the GenAI4EU initiative, and the establishment of a European AI Research Council.

The AI Act, which took effect on 1 August 2024, will become fully applicable in two years, with phased implementation of its provisions, including prohibitions and rules for general-purpose and embedded AI systems ([→eucrim 2/2024, 92–93](#)). (AP)

## Digital Space Regulation

### Overview of the Latest Developments Regarding the Digital Services Act – September to October 2024

*Eucrim* has regularly reported 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 developments concerning the DSA in the form of a chronological overview. For an overview of the developments from April 2024 to August 2024 [→eucrim 2/2024, 91–92](#).

■ 3 September 2024: The European Commission sends [reasoned opinions](#) to Czechia, Cyprus, and Portugal for not meeting their obligations under

the Digital Services Act (DSA). Despite prior formal notices in April 2024, these countries have yet to empower their Digital Services Coordinators or establish rules on penalties for DSA breaches. The DSA requires Member States to designate independent authorities by 17 February 2024 to oversee its implementation and ensure users' rights, such as filing complaints against platforms. The Commission gives the Member States two months to take corrective action. If they fail to comply, the Commission plans to refer the cases to the Court of Justice of the European Union.

■ 20 September 2024: NKL Associates s.r.o., a Czech company, brings an [action](#) against the European Commission before the General Court of the European Union. The case concerns Art. 39(1) of the DSA, which requires Very Large Online Platforms (VLOPs) displaying advertisements to maintain a publicly accessible repository containing detailed information about their ads for the duration of the ads and one year after their last display. NKL Associates argues that this obligation violates the rights of the company and its advertisers under the EU Charter of Fundamental Rights, specifically: confidentiality and privacy (Arts. 7 and 8), right to conduct business (Art. 16) and the right to property (Art. 17). The applicant requests the partial annulment of the Commission's decision enforcing this obligation and the inapplicability of Art. 39(1) of the DSA regarding the repository requirements. It also seeks reimbursement of its legal costs.

■ 4 October 2024: The European Commission publishes the [Digital Fairness Fitness Check](#), assessing the effectiveness of EU consumer protection laws in the digital era. While current laws like the Unfair Commercial Practices Directive and Consumer Rights Directive remain vital, the evaluation reveals the unique challenges posed by harmful practices in the dig-

ital space. The report emphasizes the role of the DSA in prohibiting unfair practices on online platforms. Harmful behaviors, such as dark patterns, addictive service designs, and exploitative personalized targeting, undermine consumer trust and cost EU consumers €7.9 billion annually. The DSA's provisions are highlighted as a key tool for addressing these issues, ensuring clearer standards and enforcement. The Commission calls for stronger, coordinated enforcement of the DSA and other consumer laws to tackle fragmented national approaches and provide regulatory certainty. Simplified rules, coherent application, and fairer online environments are central to the Commission's agenda for the upcoming mandate.

■ 31 October 2024: The European Commission [opens](#) formal proceedings against the Chinese online marketplace *Temu* under the DSA to investigate potential violations, including the sale of illegal products, addictive service designs, recommendation system practices, and compliance with data access obligations for researchers. The inquiry focuses on *Temu*'s efforts to prevent the sale of non-compliant goods, mitigate risks from addictive design features, ensure transparency in recommender systems, and provide researchers access to public data. As a designated Very Large Online Platform, *Temu* is subject to strict DSA obligations. The investigation follows preliminary analyses and input from national authorities, with the Commission emphasizing that the opening of proceedings does not determine the outcome. (AP)

### Latest Developments Regarding the Digital Markets Act

*Eucrim* has been regularly reporting 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 Markets



Act (DMA) aims to ensure contestable and fair markets in the digital sector. It regulates gatekeepers, which are large digital platforms that provide an important gateway between business users and consumers, whose position can grant them the power to act as bottlenecks in the digital economy. The following is an overview of the latest developments that follows on from the news on the DMA in →[eucrim 2/2024, 95–96](#).

■ 16 October 2024: The European Commission [concludes](#) that the online social networking service of X does not qualify as a core platform service under the DMA. Following an in-depth market investigation initiated on 13 May 2024, the Commission reviewed X’s rebuttal arguments and stakeholder input. Despite meeting the DMA’s quantitative thresholds, X’s service is not deemed an important gateway for businesses to reach end users. The Commission, after consulting with the Digital Markets Advisory Committee, determines that X should not be designated as a gatekeeper. It will continue monitoring market developments related to X’s service and may revisit the decision if significant changes occur. A non-confidential version of the decision will be available on the [Commission’s DMA website](#).

■ 1 November 2024: Apple publishes a [compliance report](#) outlining the company’s measures to align iOS, iPadOS, Safari, and the App Store with EU regulations. Apple emphasises that these platforms are designed as integrated systems to ensure user safety, security, and privacy. However, to comply with the DMA, Apple has implemented changes that introduce new risks, including potential exposure to malware, fraud, and harmful content. To mitigate these risks, Apple has introduced safeguards such as notarisation for iOS and iPadOS apps, authorisation processes for marketplace developers, and disclosures regarding alternative payment methods. Despite these

measures, Apple acknowledges that some risks persist and expresses a commitment to developing additional protections over time. The company is also in ongoing discussions with the European Commission to address concerns related to non-compliance investigations concerning iOS, with plans to extend any resulting changes to iPadOS as applicable.

■ 4 November 2024: The European Commission [investigates](#) whether Apple’s iPadOS meets obligations under the DMA. Designated as a gatekeeper in April 2024, Apple must allow users to set default web browsers, support alternative app stores, and enable effective access to iPadOS features for accessory devices like headphones and smart pens.

■ 11 November 2024: Bytedance Ltd [appeals](#) the General Court’s July 2024 judgment upholding its designation as a gatekeeper under the DMA (→[eucrim 2/2024, 95–96](#)). The appeal alleges legal errors in the Court’s interpretation of the DMA and procedural breaches by the European Commission. Bytedance challenges the application of DMA Arts. 3(1) and 3(5), claiming the Court misapplied criteria for market impact, gateway roles, and contestability. It states that the Court failed to holistically assess evidence and improperly dismissed key arguments. The appeal also cites violations of Bytedance’s rights of defence, arguing that procedural errors by the Commission should have led to the annulment of its decision.

■ 14 November 2024: Booking Holdings Inc. (BHI), designated as a gatekeeper under the Digital Markets Act (DMA) in May 2024, must now ensure that its platform, [Booking.com, complies with all relevant DMA obligations](#). This brings significant changes for businesses using Booking.com, such as hotels and car rental providers, including the following: freedom to offer different prices and conditions on their own websites or other channels as

“parity” clauses are banned; protection from punitive actions like increased commissions or de-listing for offering better deals elsewhere; access to real-time data generated on Booking.com, with the ability to transfer this data to other platforms. Booking must submit compliance reports, including details of its consumer profiling techniques, as required by the DMA. The European Commission will review these measures and gather stakeholder feedback.

■ 22 November 2024: The European Commission [concludes](#) its antitrust investigation into allegations of Apple’s anticompetitive practices related to certain terms imposed on e-book and audiobook app developers using its App Store within the European Economic Area. (AP)

## Institutions

### [European Court of Justice \(ECJ\)](#)

#### [Personnel Changes at the Court of Justice of the EU](#)

In the fourth quarter of 2024, the Court of Justice of the European Union (CJEU) underwent a major [change of personnel](#), with a number of Judges and Advocates-General reaching the end of their term of office, being re-elected, or newly appointed.

At the beginning of October 2024, Belgian judge [Koen Lenaerts was re-elected](#) by his peers as President of the CJEU for the period from 8 October 2024 to 6 October 2027. Furthermore, German judge [Thomas von Danwitz was elected Vice-President](#) of the CJEU, succeeding [Lars Bay Larson](#).

In addition, the following changes took place at the Court of Justice (ECJ):

■ The terms of office of five ECJ Judges were renewed, namely those of [Constantinos Lycourgos](#), [Jan Passer](#), [Thomas von Danwitz](#), [Ineta Zieme-](#)

le, *Irmantas Jarukaitis*, and *Andreas Kumin*.

- Six new Judges were appointed, namely *Bernardus Smulders* (the Netherlands, replacing *Alexandra Prechal*), *Masimo Condinanzi* (Italy, replacing *Lucia Serena Rossi*), *Fredrik Schalin* (Sweden, replacing *Nils Wahl*), *Stéphane Gervasoni* (France, replacing *Jean-Claude Bonichot*), *Niels Fenger* (Denmark, replacing *Lars Bay Larsen*) and *Ramona Frendo* (Malta, replacing *Peter George Xuereb*).

- The Presidents of the Chambers of five Judges of the ECJ were elected for a period of three years: *François Biltgen*, *Küllike Jürimäe*, *Constantinos Lycourgos*, *Irmantas Jarukaitis*, and *Maria Lourdes Arastey Sahún*.

Personnel changes concerning the Advocate-Generals of the ECJ included:

- The term of office of *Jean Richard de la Tour* was renewed.

- *Dean Spielmann* (Luxembourg, replacing *Anthony Michael Collins*), *Andrea Biondi* (Italy, replacing *Giovanni Pitruzzella*) and *Rimvydas Norkus* (Lithuania, replacing *Priit Pikamäe*) were appointed Advocates-General of the ECJ.

- *Maciej Szpunar* was [re-elected](#) by his peers as First Advocate-General of the ECJ for the period from 8 October 2024 to 6 October 2027.

At the General Court of the EU (GC), the following changes in personnel took place:

- Following the appointment of *Dean Spielmann* and *Fredrik Schalin* as Members of the Court of Justice and the end of their term of office at the GC, the Judges of the General Court [elected](#) from among their number *Roberto Mastroianni* (Italy) and *Petra Škvařilová-Pelzl* (Czechia) as Presidents of Chambers for the period from 9 October 2024 to 31 August 2025.

Furthermore, *Hervé Cassagnabere* (France, replacing *Stéphane Gervasoni*) and *Raphaël Meyer* (Luxembourg, replacing *Dean Spielmann*) were appointed as Judges of the GC. (CR)

## European Public Prosecutor's Office (EPPO)

### AG Gives Opinion on Judicial Review of EPPO's Procedural Acts

**spot light** On 4 October 2024, Advocate-General *Anthony Michael Collins* delivered his [opinion](#) in case [C-292/23](#) (*European Public Prosecutor's Office v I.R.O., F.J.L.R.*). It is the second case before the ECJ that concerns the interpretation of [Regulation 2017/1939](#) implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ("the EPPO Regulation"). The case at issue is a request for a preliminary ruling from the *Juzgado Central de Instrucción n° 6 de la Audiencia Nacional* (Central Court of Preliminary Investigation No 6 of the National High Court, Spain) and targets the interpretation of Art. 42(1) of the EPPO Regulation headed "judicial review".

#### ► Facts of the case and legal question

The case concerns an appeal of the accused persons against the legality of witness summonses. The summonses in question had been issued by a European Delegated Prosecutor (EDP) to two third parties to attend as witnesses at the criminal trial of the accused. While summonses issued by national public prosecutors provide for the possibility of an appeal under Spanish law, Spanish law does not foresee an appeal where an EDP issues such summonses. Therefore, the Spanish court referred the case to the Court of Justice asking whether this situation – the unreviewable character of the EDP measure under national law – is compatible with, *inter alia*, Art. 42(1) of the EPPO Regulation, read against the background of Art. 47 of the Charter of Fundamental Rights of the EU, the second subparagraph of Art. 19(1) TEU, and the principles of equivalence and effectiveness.

Art. 42(1) of the EPPO Regulation states that "[p]rocedural acts of the

EPPO that are intended to produce legal effects vis-à-vis third parties shall be subject to review by the competent national courts in accordance with the requirements and procedures laid down by national law."

#### ► The Advocate General's opinion

In his opinion, Advocate-General (AG) *Collins* pertains to the question of whether the ordered summoning of the third parties as witnesses is a "procedural act of the EPPO that is intended to produce legal effects vis-à-vis third parties" in the sense of Art. 42(1) of the EPPO Regulation. It thus falls to be determined whether the aforementioned summonses have legal effect vis-à-vis the accused, a scenario that would constitute a violation of Art. 42 of the EPPO Regulation, Art. 47 CFR, and other principles of EU law.

AG *Collins* first argues that said term in Art. 42(1) is an autonomous concept of EU law which requires that it be interpreted in a uniform manner throughout the European Union.

Second, he states that the concept of "acts intended to produce legal effects vis-à-vis third parties" must be interpreted in accordance with the same criteria as developed for Art. 263 TFEU – the EU's primary law provision that makes it possible to take action before the CJEU challenging the legality of EU legal acts. The AG takes the view, however, that the question as to whether a decision by an EDP to summon a third party to appear as a witness is a procedural act intended to produce legal effects vis-à-vis a person under investigation cannot be assessed and answered in a general and an abstract manner. He proposes that the ECJ should not take a general position on the question, but it is rather for the national court to examine the substance of the decision and assess its effects in the light of objective criteria, such as its content, taking into account, as appropriate, the context in which

it was made and the powers of the body that adopted it.

If the national court were to find the decision in question is an act that falls within the scope of Art. 42(1) of the EPPO Regulation, the decision must be subject to judicial review. The type of judicial review (direct or indirect) must respect the principles of effectiveness and equivalence. (CR) ■

### EPPO's Operational Activities: July – September 2024

This news item provides an overview of the EPPO's main operational activities from 1 July 2024 to 30 September 2024. It continues the periodic reports of recent issues (for the latest ones →[eucrim 2/2024, 102–104](#) and →[eucrim 1/2024, 20–21](#)) and is in reverse chronological order.

■ 3 July 2024: [Investigation “Ambrosia”](#) of the EPPO in Lisbon (Portugal) dismantles an alleged €30 million VAT fraud ring trading in essential food products (including olive oil, cooking oil, and sugar). Over 230 law enforcement officers are deployed throughout Portugal, Spain, and France. On the operation day, 222 search warrants are executed, including 40 house searches, 46 company searches, searches of four law firms and 132 vehicles, leading to 11 arrest as well as the seizure of 43 cars and €120,000 in cash. The network, using a simulated international sales circuit, involved 102 companies based in Portugal, Spain, and in France. It had long been suspected of having made an undue profit of approximately €30 million, causing an equivalent damage to the Portuguese state and the EU budget.

■ 11 July 2024: At the request of the EPPO in Naples (Italy), the Italian Financial Police (Guardia di Finanza) in Naples executes a [€1.3 million freezing order](#) against four companies and their respective legal representatives, who were suspected of fraud, embezzlement and money laundering. Based on fictitious data and forged docu-

ments, the Naples-based company with no operational headquarters, no employees, and no utility contracts, had obtained EU funding for two projects: one loan for “the development of e-commerce for SMEs (small and medium-sized enterprises) in foreign countries” with an total value of €300,000 (of which €150,000 was disbursed); the second project involved a €1.3 million grant for SMEs (the money was almost fully disbursed and financed by the Recovery and Resilience Facility (RRF)).

■ 12 July 2024: At the request of the EPPO in Milan (Italy), the Italian Financial Police (Guardia di Finanza) executes a €5,039,260 freezing order against a company suspected of major customs fraud involving the importation of [e-bikes from China](#). The company is alleged to have evaded payment of anti-dumping duties, customs duties, and VAT amounting to more than €9.8 million by importing these e-bikes into the EU in parts and in separate consignments. The amount in the freezing order corresponds to the tax allegedly evaded.

■ 15 July 2024: A fraud investigation of the EPPO in Turin (Italy) leads to the arrests of two suspects. In addition to the arrests, the Italian authorities execute a €1.3 million freezing order, seize five properties with a total value of over €1 million, and freeze five bank accounts with a total value of €213,000. The suspects had received loans guaranteed by the European Investment Fund [for the development of drones](#) for commercial use. In order to obtain these loans, the suspects allegedly submitted false balance sheets and falsified accounting documents.

■ 17 July 2024: [Investigation “Easy Car”](#) by the EPPO in Milan (Italy) leads to the arrest of two suspects and the execution of a freezing order against seven companies under investigation for a major intra-community VAT carousel fraud involving luxury cars. The

suspects are alleged to have evaded €7.6 million in VAT payments on new car registrations by falsifying the origin of the vehicles.

■ 19 July 2024: Investigations of the EPPO in Venice (Italy) uncover an alleged €8.8 million VAT carousel fraud involving the trade in [cleaning products and alcoholic and non-alcoholic beverages](#). A variety of fraudulent tactics, including fake invoices, fictitious transactions, and missing traders, had been used to claim fraudulent VAT reimbursements from national tax authorities. Products were also on sale at artificially low prices, thereby undercutting legitimate competitors.

■ 25 July 2024: Suspicions of procurement fraud, misappropriation of EU funds, and corruption prompt the EPPO in Nicosia (Cyprus) to launch an investigation into a project to create a [natural gas entry point for Cyprus](#). The construction of the liquefied natural gas (LNG) import terminal, which would allow Cyprus to connect to the wider European gas market, is costing €542 million, of which around €101 million are financed by the Connecting Europe Facility (CEF) programme.

■ 26 July 2024: The EPPO in Bratislava (Slovakia) opens an investigation into [attempted fraud of EU funds in connection with the construction of a waste treatment plant](#). A comparison between the project documents submitted for the planning permission procedure and those submitted for the grant application had revealed discrepancies contrary to the requirements set out in the call for grant applications.

■ 26 August 2024: The EPPO in Sofia (Bulgaria) is investigating a €2.6 million EU-funded project to reconstruct the water supply network and [the water reservoir of a municipality in Bulgaria](#). Public officials from Bulgaria's State Fund for Agriculture are suspected of having made fraudulent arrangements with a mayor and the private companies to inflate the price of the works

and overcharge the paying agency. The public officials are also alleged to have drawn up documentation containing false information, certifying that all the works were completed on time. EPPO investigators had uncovered evidence of fraud in the execution of the contract, which had been awarded to private companies.

- 29 August 2024: The EPPO in Vilnius (Lithuania) expands its investigation into a former assistant of a Lithuanian Member of the European Parliament (MEP) ([→eucrim 1/2024, 20–21](#), entry on 29 March 2024) to the MEP himself. The [former Lithuanian MEP](#) is now officially suspected of abuse of office, falsification and use of false documents, illegal acquisition, possession and use of an electronic document as well as the acquisition of high value foreign assets.

- 4 September 2024: The EPPO in Frankfurt am Main (Germany) is investigating three social enterprises that received more than €6.6 million in grants from the European Social Fund (ESF) and the European Social Fund Plus (ESF+) for [projects to help unemployed people](#) with particular difficulties accessing the labour market. The five suspects, all managers and employees of the social enterprises, are alleged to have submitted documents containing false information on the allocation of staff to the projects in order to obtain a higher amount of funding for their companies. Employees were allegedly pressured to sign forms stating that they had worked on certain ESF projects when in fact they had not.

- 12 September 2024: The EPPO in Athens (Greece) is investigating a [€30 million VAT fraud and money-laundering scheme](#). To evade VAT, the suspects had set up a complex web of companies in Greece and other EU Member States (Cyprus and Slovakia) to trade small electronic goods through a fraudulent chain of missing traders. The investigation has

also uncovered a number of fraudulent schemes involving additional VAT evasion and money laundering amounting to several million euros, which will be further investigated.

- 24 September 2024: At the request of the EPPO in Rome (Italy), the Italian Financial Police (Guardia di Finanza) of Giulianova (Teramo) executes a freezing order amounting to €114,000 against an Italian company, which operates wholesale trade of food and tobacco. The company was granted €228,000 funding from the Recovery and Resilience Facility (RRF) [for the development of an e-commerce platform](#). The grant application was allegedly based on falsified financial statements. Half of the granted amount (€114,000) was already disbursed.

- 25 September 2024: The EPPO in Cluj-Napoca (Romania) has several public and private places searched based on an investigation into [procurement fraud, forgery of documents and abuse of office](#). Under suspicion are several civil servants of the Maramureş County which received funding of €1 million under the RRF for the renovation of a public administration building. (CR)

## [Europol](#)

### [First Operation with Ameripol](#)

In the [first ever joint operation](#) between Europol and the Specialised Cybercrime Centre of Ameripol (an organisation for police cooperation in the Americas, currently made up of 33 police forces in 27 countries), an international criminal network was dismantled that had been running a phishing-as-a-service platform for unlocking mobile phones. In five years of operation, more than 2,000 unlockers registered and used the services to unlock more than 1.2 million phones, affecting more than 480,000 victims worldwide. (CR)

## [Europol Intensifies Cooperation with the ICC](#)

Europol and the International Criminal Court (ICC) [signed two further legal instruments](#) on 18 September 2024, implementing their working arrangement of 25 April 2023 ([→eucrim 1/2023, 22–23](#)). The new Liaison Officer Agreement allows the ICC to nominate a liaison officer to Europol. In addition, a new Memorandum of Understanding now enables the ICC to be connected to Europol's communication platform SIENA, allowing for the secure exchange of sensitive operational information.

Since the new Europol Regulation came into effect in May 2017, Europol aims to facilitate the cooperation and coordination of EU Member States and Third Parties' efforts to identify and investigate individuals, networks and groups involved in committing core international crimes through its Analysis Project. In particular, Europol provides analytical support, streamlines information exchange, carries out online monitoring, and provides open sources intelligence. Since 2023, cooperation with the ICC has intensified. (CR)

## [Eurojust](#)

### [Eurojust: New President and Vice-President](#)

On 12 November 2024, *Michael Schmid* was elected [new President of Eurojust](#) for a four-year term. Mr Schmid succeeds *Ladislav Hamran*, who has completed his second and final term of office. Mr Schmid has previously served as National Member and Deputy National Member of Eurojust for Austria and Justice Counsellor at the Permanent Representation of Austria at the EU in Brussels. The President of Eurojust represents the Agency and oversees the meetings of the National Members who meet regularly in the College. The President



also directs and monitors Eurojust's activities and management.

On 10 December 2024, *Mr José de la Mata Amaya*, [National Member for Spain, was elected Vice-President of Eurojust](#). His four-year mandate started on 18 December 2024. Eurojust's two Vice-Presidents (Mr de la Mata's fellow is *Ms Margarita Šniutytė-Daugėlienė*) carry out duties entrusted to them by the President of the Agency and represent or replace him. As the new Vice-President, Mr de la Mata will also be a member of Eurojust's Executive Board, which assists the Agency's College in its management tasks and supervises the preparatory work of the Administrative Director. He succeeds former Vice-President *Boštjan Škrlec*, National Member for Slovenia at Eurojust, who decided not to run for a second mandate. Mr de la Mata has been Eurojust's National Member for Spain since December 2020. (CR)

### [Eurojust Agreement with Bosnia and Herzegovina Signed](#)

On 24 October 2024, the European Commissioner for Justice, *Didier Reynders*, and the Minister of Justice of Bosnia and Herzegovina (BiH), *Davor Bunoza*, [signed a cooperation agreement on Eurojust](#) to increase the efficiency of investigations and prosecutions in the fields of organised crime, terrorism, trafficking in human beings, cybercrime, and other transnational criminal activities. Under the agreement, BiH will be able to post a liaison prosecutor to Eurojust, enabling direct participation in joint investigations and access to Eurojust's operational tools. The next steps are for the agreement to be ratified and for BiH to adopt a new law on personal data protection in line with EU standards.

The Eurojust agreement is a further key step for BiH's integration into the EU law enforcement and judicial cooperation framework. BiH already concluded an operational and strategic cooperation [agreement with Europol](#)

and a working arrangement with the European Public Prosecutor's Office ([→eucrim 4/2023, 321–322](#)). (CR)

### [Fake Investment Platforms Dismantled](#)

At the end of October 2024, a joint investigation team investigating a [large-scale online investment scam](#) involving players in Germany, Serbia, and Cyprus led to the seizure of computer equipment, hard drives, mobile phones, and digital data as well as the arrest of a suspect in Cyprus through a coordinated action. The perpetrators allegedly ran a fraud scheme using fake investment platforms that promised high returns for low investments. While 120 known victims in Germany have lost around €12 million, investigations suggest that there are victims worldwide, with the total fraud amounting to at least €300 million or even as much as €500 million. Investigations were promoted by a Joint Investigation Team between Germany and Serbia. Eurojust assisted in setting up the Team. (CR)

### [Forged Works of Contemporary Art Seized](#)

At the beginning of November 2024, a long-running investigation being conducted by Italian, Belgian, French, and Spanish authorities, supported by Eurojust, dismantled a [European forgery network](#) that had counterfeited contemporary art, including works by famous artists such as Banksy, Andy Warhol, Pablo Picasso, Joan Miró, Francis Bacon, Wassily Kandinsky, Gustav Klimt, Claude Monet, Vincent van Gogh, and Salvador Dalí. The network had faked more than 2,000 works of art, along with forged certificates and stamps of authenticity, in order to sell them at several complicit auction houses in Italy. Following the take-down, 38 people were charged with conspiracy to forge and deal in contemporary art. Had the pieces been auctioned, the estimated economic

damage would have been around €200 million. Eurojust supported the operation *inter alia* by coordinating European Investigation Orders against suspects in Spain, France, and Belgium. (CR)

### [European Judicial Network \(EJN\)](#)

#### [Fiches Belges for Montenegro and Serbia Available](#)

In order to assist legal practitioners in preparing their requests for mutual legal assistance (MLA) to Montenegro and Serbia, the EJN has [launched](#) the EJN [Fiches Belges for Montenegro and Serbia](#) on its website. The Fiches Belges provide information on the legal systems and criminal procedures of these countries. They outline the applicability of all investigative measures that could be requested by an MLA and any additional national procedural requirements for the execution of such requests. They are available since November 2024. Integrating information of the legal systems of Western Balkan countries on the EJN website is one of the EJN's current key initiatives. (CR)

### [Frontex](#)

#### [Frontex Signs Agreement with UNHCR](#)

On 17 September 2024, [Frontex and the UNCHR \(the UN Refugee Agency\) signed an agreement](#) to strengthen their cooperation on border management and humanitarian protection across Europe. The agreement allows the two organisations to exchange information and expertise to promote and support effective border management.

Cooperation under the agreement will focus on capacity building and training, information sharing and coordination, and complementary communication.

The organisations will share expertise to ensure that border management



is both effective and compliant with international human rights and refugee law. Communication between Frontex and the UNHCR will be enhanced to enable timely and accurate responses to border operations. Lastly, both parties will promote a consistent approach to addressing public concerns on migration, border security, and refugee protection. (CR)

## Specific Areas of Crime

### Protection of Financial Interests

#### Recast of Financial Regulation in Force

**spot light** On 26 September 2024, the revised Regulation on the financial rules applicable to the general budget of the Union (“the Financial Regulation”) was [published in the Official Journal](#). It has been applicable as from 30 September 2024. The Financial Regulation lays down the principles and procedures governing the establishment and implementation of the general budget of the European Union and Euratom. In addition it includes the provisions for the presentation and auditing of their accounts.

The recast of the Financial Regulation was proposed by the European Commission on 16 May 2022 ([→eucrim 2/2022, 105](#)). The Council and the European Parliament reached a [provisional agreement](#) at the trilogue in December 2023. The new Financial Regulation is a targeted revision to align the rules with the multiannual financial framework (MFF) 2021–2027. It also includes targeted improvements for the protection of the EU’s financial interests ([→eucrim 2/2022, 105](#)). The main changes include the following:

- The Financial Regulation follows the “single rulebook” approach by reflecting certain derogations from the budgetary principles set out in the sectoral basic acts;

- The EU’s financial interests are better protected by limiting additional administrative burdens for national administrations and by safeguarding data protection in the process of digitalisation;

- The crisis management will be improved by enabling EU institutions or bodies to procure on behalf of Member States or to act as a central purchasing body, to donate or resell supplies and services;

- Regarding the EU budget in general, the Financial Regulation introduces the concept of negative revenues as a solution until the end of the current MFF for the financing of negative interests stemming from the reduction or annulment of competition fines;

- Rules and procedures are simplified, to improve legal certainty and clarity for recipients, while reducing administrative burden for applicants. The Financial Regulation is the EU’s main point of reference for the general budget. It is foreseen that the Regulation is reviewed whenever it proves necessary to do so and in any case at the latest two years before the end of each multiannual financial framework. (TW)

#### ECA: Increasing Error Rate in EU Spending and Growing Debts Are Cause for Concern

The rate of error in EU budget spending has again increased in 2023 compared to previous years. And the rising financial burdens due to record levels of debt, including the Russian war of aggression against Ukraine and high inflation, are a cause for concern. These are the main findings in the [European Court of Auditors’ \(ECA\) annual reports on the implementation of the EU budget](#) and on the activities funded by the European Development Funds (EDFs) for the 2023 financial year, which were presented on 10 October 2024. For the reports for 2022 [→eucrim 3/2023, 251–252](#), and for 2021, [→eucrim 3/2022, 183–184](#).

The EU auditors stated that the revenue can be considered error-free. In 2023, EU payments amounted to a total of €239.2 billion: €191.2 billion in expenditure from the EU budget and a further €48 billion in expenditure under the Recovery and Resilience Facility (RRF) – the EU’s main source for recovering from the COVID-19 pandemic. The EU auditors expressed concern that the error rate for the expenditure from the EU budget had risen to 5.6% (2022: 4.2%, 2021: 3%). In conclusion, the estimated level of error was material and pervasive, and thus an adverse opinion on the EU’s spending in 2023 had to be issued. The auditors emphasised that the significant increase in the estimated error rate is largely due to the errors found in cohesion expenditure (rate of 9.3% compared to 6.4% in 2022). One reason for this increase is that national administrations spend money from competing EU funds under time pressure.

The ECA also pointed out that it reported fraud cases to OLAF and the EPPO. During audits conducted in 2021 and 2022, the ECA reported 20 (in 2022: 14) cases to OLAF, and 17 to the EPPO. From these reports, OLAF opened four investigations and the EPPO nine investigations. During audits of 2023 expenditure, the ECA already identified 12 cases of suspected fraud. The most frequent grounds for the suspicion of fraud were:

- Intentional use or presentation of false, incorrect or incomplete statements or documents and/or non-disclosure of information in violation of a specific obligation, resulting in the misappropriation or wrongful retention of EU funds;

- Artificial creation of conditions necessary for EU financing;

- Use of grants for unauthorised purposes.

With regard to RRF expenditure, the ECA issued a “qualified opinion” as last year. This means that problems

have been identified, but are not pervasive. It was found that around one third of the RRF grant payments in 2023 did not comply with the rules and conditions. In addition, the RRF mechanism is still affected by system weaknesses.

Lastly, the ECA emphasised that the EU budget is coming under increasing pressure. Next to the high inflation rates and the increasing financial support to the Ukraine, growing debts are concerning: The total amount of outstanding commitments reached a record high of €543 billion by the end of 2023 (in 2022: €452.8 billion). Meanwhile, EU debt jumped to €458.5 billion in 2023 (in 2022: €348 billion, or +32 %). The main reason is the borrowing for the Next Generation EU (NGEU) of €268.4 billion. EU debt is now twice as high as in 2021 (when it stood at €236.7 billion). This means that the EU is now one of the largest debt issuers in Europe, even though it is unclear whether the Commission's own resources proposal will generate sufficient revenue to repay NGEU debt, the ECA report says. (TW)

### ECA: Double Funding with EU Money is a Blind Spot

**spot light** On 21 October 2024, the European Court of Auditors (ECA) published a [special report on double funding from the EU budget](#). It is of the opinion that the risk of EU funds being spent twice on the same measure is increasing, while the existing control mechanisms are not sufficient to reduce the higher risk of double funding.

As part of this audit, the ECA assessed the Commission's and Member States' systems to avoid double funding from the Recovery and Resilience Facility (RRF) on the one hand and from the Cohesion Policy Funds and the Connecting Europe Facility on the other. The auditors noted that corresponding measures in similar areas

such as transport and energy infrastructure are financed from both the EU budget and the RRF. The increasing risk of double funding is corroborated by the fact that the Commission identified the first two potential cases of double funding involving RRF money in a Member State which indicates that the tools available are neither suitable for nor effective at detecting double funding. The main shortcomings to mitigate the risks of double funding were identified as follows:

- The EU legal framework, especially the definition of double funding, has not been adapted to the peculiarities of the RRF which is not linked to costs but rather reward the fulfilment of milestones and targets.

- Minimum control requirements have not been specified and there are uncertainties about which checks could address the risk of double funding effectively.

- Member States face problems with several layers of governance and audits are carried out differently. The fragmented IT landscape prevents effective cross-checks and the limited use of Arachne and other data mining tools or project databases makes double funding difficult to detect.

- The assurance the Commission is able to provide on the absence of double funding relies on limited evidence. This is due to a blind spot in the RRF design itself, which results in an accountability gap.

In particular, the ECA recommends that the Commission should strengthen controls on zero-cost measures, improve coordination between funding programmes and instruments using financing not linked to costs, and set up/use integrated and interoperable IT systems and data mining tools for all funding programmes and instruments.

This audit presented in the special report also draws on other [RRF-related reports, reviews and opinions](#) which the ECA has published in recent years and months. (TW)

### ECA Assessed EU Funding for Digitalisation of Healthcare

EU support for Member States to digitalise their healthcare systems was overall effective, but EU funds were difficult to use due to the number of different rules. These are the main findings in the [European Court of Auditor's \(ECA's\) Special Report No 25/24](#) which was released on 20 November 2024.

The ECA's audit assessed not only whether the EU policy framework provided Member States with clear objectives and support, but also whether the Commission helped EU countries to identify and use the EU funds available to finance e-health projects, and monitored progress in healthcare digitalisation, including the use of EU funds by the Member States. The report voiced overall satisfaction with the promotion of the digitalisation of healthcare during the 2014–2020 and 2021–2027 programming periods so far. The auditors found that the Commission provided effective support and guidance overall, and the audited projects in the selected countries (Spain, Malta and Poland) contributed to the digitalisation of healthcare.

However, given that different EU programmes with different rules finance projects on healthcare digitalisation, made it difficult for some Member States to identify the EU funds available, and created obstacles for them when applying for funding. Problems further arose because neither the Commission nor most Member States have a comprehensive overview of the EU funds used for healthcare digitalisation projects. As a result, it has been difficult to establish the extent of EU financial support in the Member States. Shortcomings also existed with regard to the tracking of progress in healthcare digitalisation, in particular due to different methodologies applied for indicators and benchmarks.

The ECA recommended that the Commission should especially improve its reporting on the use of EU

funds for healthcare digitalisation across the various financing programmes by 2026.

ECA's Special Report 25/24 is connected to its [2019 report on EU actions for cross-border healthcare](#). In its 2019 report, the ECA concluded that although EU actions in cross-border healthcare enhance Member States' collaboration, the benefits for patients were limited. (TW)

## Tax Evasion

### ECJ Strengthens Legal Professional Privilege in the Exchange of Tax Information

**spot light** On 26 September 2024, the ECJ handed down an [important judgment](#) on the extent of the protection of the confidentiality of lawyer-client communication in the cross-border exchange of information on tax matters. The ECJ ruled that the Luxembourgish legislation under which advice and representation by a lawyer in tax matters do not enjoy the strengthened protection of communications between lawyers and their clients is incompatible with Art. 7 of the Charter of Fundamental Rights of the EU (CFR).

#### ► Facts of the case and questions referred

In the case at issue ([Case C-432/23, Ordre des avocats du Barreau de Luxembourg](#)), F SCS, a law firm incorporated as a limited partnership in Luxembourg, defends itself against a decision to provide information issued by the *administration des contributions directes* (Luxembourg Inland Revenue). This decision followed a request by a Spanish tax authority, which seeks information concerning the services F SCS provided to K, a company incorporated under Spanish law, in connection with the acquisition of a business and a majority shareholding in a company, both also incorporated under Spanish law.

After F SCS refused to disclose information, the Luxembourg Inland Revenue imposed a fine. In the action for annulment of this decision, F SCS – supported by the Luxembourg Bar Association – argued that the Luxembourgish legislation under which it is obliged to provide the authorities with all documentation and information relating to the lawyer's relationship with his or her client does not respect the legal professional privilege. F SCS also stated that the instruction from its client in the case to which the decision relates did not cover tax matters but concerned only company law; this is a ground for lawyers to refuse disclosure of information entrusted to them in the exercise of their profession, as foreseen in Article 177(1) of the *loi générale des impôts du 22 mai 1931* (General Tax Law of 22 May 1931), known as the "Abgabenordnung" (AO).

By contrast, the Luxembourg Inland Revenue referred to Article 177(2) AO, which provides that the refusal ground is not applicable in respect of facts of which lawyers became aware in connection with advice or representation in tax matters, unless an affirmative or negative response to questions would put their clients at risk of criminal prosecution.

The *Cour administrative* (Higher Administrative Court, Luxembourg), before which F SCS's action for annulment is pending, observed that both the underlying EU law (Council [Directive 2011/16/EU](#) on administrative cooperation in the field of taxation) and the national law could be incompatible with fundamental rights. It especially wonders whether the ECJ's statements made in its 2022 [judgement in Case C-694/20](#) (*Orde van Vlaamse Balies and Others*) are applicable also to the present situation. In *Orde van Vlaamse Balies*, the ECJ ruled that the obligation for a lawyer under [Art. 8ab of Directive 2011/16](#) (as amended by Directive 2018/822) to inform other intermediaries involved in potential-

ly aggressive cross-border tax-planning infringes the right to respect for communications with his or her client. Against this background, the *Cour administrative* posed questions on the following three issues:

- Scope of the right to respect for communications between lawyers and their clients guaranteed by Art. 7 CFR;
- Validity of Directive 2011/16 in the light of Art. 7 and Art. 52(1) CFR;
- Compatibility of the administrative decision such as that at issue in the main proceedings with Art. 7 and Art. 52(1) CFR.

#### ► Interference with right to respect lawyer-client communication

The ECJ clarifies: Legal advice on company law is subject to the strengthened protection of communications between lawyers and their clients guaranteed by European fundamental rights.

The ECJ emphasises the scope of the protection of professional secrecy guaranteed by Art. 7 CFR, which corresponds to the protection guaranteed by Art. 8(1) ECHR, both in terms of the existence and the content of the mandate. The reason for the protection of professional secrecy is the fundamental task entrusted to lawyers in a democratic society, namely defending litigants. It follows that legal advice given by a lawyer, regardless of the area of law to which it relates, is guaranteed the protection of Art. 7 CFR with regard to lawyer-client communication. An instruction to a lawyer to provide the administration with all documents and information concerning his relations with his client in the context of advice on company law constitutes an infringement of that guarantee.

#### ► Validity of Directive 2011/16

The ECJ argues: The fact that the EU directive does not contain any provisions on the protection of the confidentiality of communications between a lawyer and his client in the context of the requested Member State's obligation to provide information does not

mean that the directive infringes Arts. 7 and 52(1) CFR.

In view of those provisions, the European legislature merely defined the obligations of the Member States in relation to each other for the purposes of the exchange of information provided for in the directive, while authorising them not to comply with a request for information where conducting the investigations sought or gathering the information concerned would be contrary to their legislation. Accordingly, it is the responsibility of the Member States to ensure that their national procedures for gathering information for the purposes of information exchange comply with the Charter, in particular Art. 7.

► *Compatibility of the national legislation and the administrative decision at issue*

The ECJ concludes: Instructions based on a national regulation under which advice and representation by a lawyer in tax matters is not covered by the strengthened protection of lawyer-client communication, except where there is a risk of criminal prosecution of the client, are in breach of Arts. 7 and 52(1) CFR.

The ECJ stresses that the Charter guarantees that persons who consult lawyers can reasonably expect their communications to remain private and confidential. Apart from exceptional situations, they must have confidence in the fact that their lawyers will not disclose the fact that they are consulting them to anyone without their agreement.

Considering these premises, the Luxembourgish legislation renders the afforded protection devoid of its very essence because it basically excludes the content of advice given by lawyers in tax matters – and thus an entire branch of law in which lawyers are likely to advise their clients. As for the decision at issue, which concerns an entire file not related to tax matters, it further extends the scope of the in-

fringement of the substance of the right protected by Art. 7 CFR. Both the national legislation and its application by means of the administrative decision are far from being confined to exceptional situations, and thus infringe the essence of the right guaranteed by Art. 7.

► *Put in focus*

Following the [judgment in Orde van Vlaamse Balies](#) (see above), the ECJ reaffirms the importance and function of legal professional privilege. The confidentiality of communication between lawyer and client is strengthened. It is clarified that legal advice or representation cannot generally be excluded from the protection afforded to legal professional privilege. The decision also means that the cross-border exchange of information between the authorities is limited in tax matters since there is no differentiation between lawyers specialized in tax or corporate law and defending criminal lawyers.

The ECJ continued however its stance that Directive 2011/16 on administrative cooperation in the field of taxation is not incompatible with higher ranking EU law (the Charter). A try to declare the Directive invalid also failed in case [C-623/22, Belgian Association of Tax Lawyers and Others](#)) which was decided on 29 July 2024 (→[eucrim 2/2024, 120–122](#)). However, the latter case concerned the newly introduced reporting obligation for aggressive tax planning.

In the present case, the ECJ did not follow [the bar associations' plea](#) that Directive 2011/16 itself is invalid since it lacks provisions on legal professional privilege. The bar associations referred to other ECJ case law (particularly with regard to data retention) in which the Court emphasised that, in order to meet the requirements of Art. 52(1) CFR, secondary EU law (i.e., a directive) must itself regulate the interferences with fundamental rights that they effect and intend, and to that end

lay down clear and precise rules as to the scope and application of the measures provided for, and imposing minimum safeguards. The ECJ seems now follow the line that in the area of cooperation against tax evasion and tax fraud, it is the national law which must provide the necessary safeguards for the protection of the legal professional privilege.

Lastly, it must also be noted that the ECJ emphasised again the protection of lawyers who are conferred a “fundamental role in a democratic society”, i.e., lawyers who give independent legal advice and act in good faith towards their clients. Comparing the [judgment in Belgian Association of Tax Lawyers](#) (see above) on the one hand and the present judgment in *Ordre des avocats du barreau de Luxembourg* as well as the judgment in *Orde van Vlaamse Balies* on the other hand, the ECJ does not extend the strengthened protection of the legal professional privilege to other professionals even if they advise in legal matters and are subject to professional secrecy. (TW) ■

**ECJ: Limiting the Interest Deduction for an Intra-group Loan Is Compatible with EU Law**

On 4 October 2024, the ECJ ruled in [Case C-585/22 \(X BV/Staatssecretaris van Financiën\)](#) that a Member State can refuse to deduct tax on interest costs with reference to abusive tax practices to the extent that the interest is not at arm's length. The [ECJ found](#) that the Dutch provisions on abusive tax practices can act as a deterrent to the exercise of freedom of establishment. However, it recognised that these legal provisions constitute a permissible restriction on the freedom of establishment and pursue a legitimate objective of combating tax evasion. This objective also applies to cases in which an entity only becomes an entity related to the same taxpayer as a result of the acquisition or increase of a shareholding (present case).



The Court also stated that the taxpayer can rebut the presumption that the interests paid constitute or form part of “wholly artificial arrangement” by comparing it with normal market conditions. In order to check whether the requirement of arm’s length is met, the economic reality of the transactions must be taken into account.

If the artificial nature of a transaction results from an unusually high interest rate on such a loan, which otherwise reflects the economic reality, the principle of proportionality requires that the proportion of this interest paid that is above the normal market interest rate be deducted. By contrary, if the loan is, in itself, devoid of economic justification and, but for the relationship between the companies and the tax advantage sought, would never have been contracted, it is consistent with the principle of proportionality to refuse the deduction of the whole interest. (TW)

#### EU and Norway: Updated Agreement on Administrative Cooperation in the Field of VAT

On 4 October 2024, the [EU and Norway signed](#) an Agreement amending the 2018 Agreement between the parties on administrative cooperation, combating fraud and recovery of claims in the field of value added tax. For the negotiations of this amending agreement → [eucrim 2/2022, 108](#). For the existing 2018 Agreement → [eucrim 1/2018, 16](#).

On 5 November 2024, the [Council of the European Union approved](#) the new agreement on behalf of the Union. The Agreement was published in the EU’s [Official Journal of 19 November 2024](#). It will enter into force two months after the parties notified each other of the completion of the internal legal ratification procedures.

The update of the 2018 agreement aimed at aligning the EU-Norway partnership with the latest EU VAT legislation. It will provide new cooperation tools, including the following:

- The spontaneous and automatic exchange of information and feedback;
- Assistance on administrative notifications;
- Participation in administrative enquiries (PAOEs);
- Simultaneous controls (MLCs);
- Enhanced use of digital tools, such as e-invoicing and the digitization of VAT reporting;
- Norway’s participation in [Eurofisc](#) (the EU’s network facilitating real-time information exchange among tax authorities to address VAT fraud across borders).

As regards recovery, the new agreement includes the requests for recovery, requests for enforcement and requests for precautionary measures. (TW)

#### Non-Cooperative Tax Jurisdictions: Antigua and Barbuda No Longer Blacklisted

On 8 October 2024, the [Council has removed Antigua and Barbuda from the EU list](#) of non-cooperative jurisdictions for tax purposes, reducing the [list to 11 jurisdictions](#): American Samoa, Anguilla, Fiji, Guam, Palau, Panama, Russia, Samoa, Trinidad and Tobago, the US Virgin Islands, and Vanuatu.

The EU list of non-cooperative jurisdictions, established in December 2017 as part of the EU’s external strategy on taxation, seeks to encourage transparency, fair taxation, and the implementation of international measures to prevent tax base erosion and profit shifting. The Council reviews the list twice a year to ensure it reflects current progress and developments (for the last revision → [eucrim 1/2024, 29](#)). These decisions are prepared by the Council’s Code of Conduct Group, which monitors tax measures in both EU Member States and international jurisdictions, working closely with the OECD Forum on Harmful Tax Practices to promote global tax governance.

Antigua and Barbuda had been added to the list in October 2023 following

a negative assessment by the OECD Global Forum on its exchange of information practices. However, after making changes to its tax rules, the Global Forum granted Antigua and Barbuda a supplementary review, which is scheduled to take place soon. While awaiting the outcome of this review, Antigua and Barbuda has been moved to the state-of-play document (Annex II), reflecting ongoing cooperation with the EU on tax matters.

In the context of the Annex II-list, Armenia and Malaysia have been removed after having fulfilling their commitments by amending a harmful tax regime.

The next update to the EU list of non-cooperative jurisdictions is scheduled for February 2025. (AP)

#### Counterfeiting & Piracy

##### EU Customs Report 2023: €3.4 Billion Worth of Counterfeit Goods Seized to Protect Single Market

On 13 November 2024, the European Commission and the European Union Intellectual Property Office (EUIPO) published their [2023 joint report](#) on the EU enforcement of intellectual property rights (IPR). In the report, the two organisations provide an overview of the work carried out by EU customs officials responsible for the enforcement of IPR, and highlight the growing need for continued action against counterfeiters. For the 2022 IPR Enforcement Report → [eucrim 4/2023, 326–327](#).

In 2023, EU customs authorities intercepted counterfeit goods worth nearly €3.4 billion. This marked a 77% increase against the previous year, with around 152 million items seized, including toys, games, and packaging materials.

The report confirmed several trends from previous years:

- For the second year in a row, “games” is the product category which was mostly detained in 2023. In the top



five product categories remain “toys”, “recorded CDs/DVDs”, and “packaging material”;

- Almost the entire total volume of detentions (98%) and the entire estimated value (over 94%) were reported by ten EU Member States; Italy remains on the top of the list in terms of detained fake items (74%) and the account for the estimated value (58%);
- As to the list of the top three countries of provenance in terms of volume of IPR infringing goods entering the EU, 2023 again showed the preponderance of China with over 56%, followed by Hong Kong with almost 9% and Turkey with over 8%.

The report highlighted the growing challenges posed by counterfeit goods, especially with the rise of e-commerce, which not only harm legitimate businesses but also endanger the health and safety of EU consumers.

In response, the European Commission proposed a comprehensive reform of the EU Customs Union, the most ambitious since its founding in 1968. The reform aims to establish an EU Customs Authority, create a new EU Customs Data Hub, and provide enhanced tools and a stronger regulatory framework for customs authorities (→[eucrim 2/2023, 158–159](#)). These measures seek to streamline information exchange, improve supply chain monitoring, and bolster consumer safety while supporting a more competitive Single Market. (AP)

## Procedural Law

### Data Protection

#### ECJ Ruled on Police Access to Mobile Phone Data

**spot light** On 4 October 2024, the ECJ, sitting as Grand Chamber, [delivered an important judgment](#) on the respect for data protection rules

if police attempt to access data on a mobile phone. The ECJ laid down parameters for such access under EU law. The ruling concerned scope and limits of the following data protection principles:

- Principle of “data minimisation”;
- Prior review by a court or independent administrative authority;
- Information to be made available or given to the data subject.

#### ► *Facts of the case and questions referred*

In the case at issue ([C-548/21, Bezirkskshauptmannschaft Landeck](#)), Austrian customs officers seized a package containing 85 grams of cannabis. Subsequently, in a police investigation relating to narcotics trafficking, two police officers conducted a search of the recipient’s (CG’s) residence and questioned him regarding the consignor of the package. Following CG’s refusal to give access to the police officers to the connection data on his mobile telephone, those officers seized the telephone. Next, an expert of the Landeck District (Austria) police station and – after his failure – experts at the Vienna Bundeskriminalamt (Federal Office of the Criminal Investigation Police) attempted in vain to unlock the telephone in order to access the data contained therein.

The Austrian police did not have an authorisation from the public prosecutor’s office or a court, and the attempts to unlock were not documented in the police files. Furthermore, CG was not informed promptly of the attempts to make use of his mobile telephone. He only became aware of the police measures during proceedings before the Landesverwaltungsgericht Tirol (Regional Administrative Court, Tyrol, Austria), the referring court, before which he challenged the lawfulness of the seizure of his mobile telephone.

Given that the criminal investigations only concerned a minor offence (punishable pursuant to the Austrian Law on Narcotics by a term of impris-

onment of up to a year only) and recalling the ECJ’s judgments in *Ministerio Fiscal* (→[eucrim 3/2018, 155–157](#)) and *Prokuratuur* (→[eucrim 1/2021, 28–30](#)), the Tyrol court sought clarification on the following three issues:

- Constitutes full and uncontrolled access to all the data contained in a mobile telephone so serious an interference with fundamental rights that this access must be limited to fighting serious offences?
- Are national legal rules precluded, pursuant to which the criminal investigation police can gain, without the authorisation of a court or independent administrative body, full and uncontrolled access to all data contained in a mobile telephone?
- Are national legal rules compatible with the right to an effective judicial remedy, in so far as they do not require the police authorities to inform the owner of a mobile telephone of the measures for the digital exploitation of that telephone?

#### ► *The applicable law*

The ECJ first countered arguments against its jurisdiction because the request for preliminary ruling erroneously referred to the [e-privacy Directive 2002/58/EC](#). The judges in Luxembourg confirmed that the Directive is indeed not applicable. If Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only, subject to the application of the [Law Enforcement Data Protection Directive 2016/680](#). This is the case here because the police attempted to directly access personal data contained in a mobile telephone, without any intervention on the part of a provider of electronic communications services having been sought.

However, the judges in Luxembourg stated that the procedure before the ECJ was lawful when the Court reformulated the questions referred in light of the relevant Directive 2016/680.

➤ *Application of Directive 2016/680*

The ECJ then rejected arguments put forward by certain governments that Directive 2016/680 is only applicable if personal data contained in a mobile telephone were successfully accessed by law enforcement authorities. The ECJ clarified that an access attempt falls within the scope of Directive 2016/680. This conclusion can be drawn from the wording, context, and objective of Art. 3 no. 2 of the Directive as well as from the principle of legal certainty: if the applicability of Directive 2016/680 were to depend on the success of the attempt to access personal data contained in a mobile telephone, that would create uncertainty incompatible with the principle of legal certainty for both the competent national authorities and individuals.

➤ *Requirements for the protection of fundamental rights*

With regard to the questions posed by the Austrian court, the ECJ examined whether national legal rules which afford the competent authorities the possibility of accessing data contained in a mobile telephone, for the purposes of the prevention, investigation, detection and prosecution of criminal offences in general, without making reliance on that possibility subject to prior review by a court or an independent administrative body, are compatible with the principle of “data minimisation”, as an expression of the principle of proportionality, enshrined in Art. 4(1)(b) of Directive 2016/680.

In this context, the ECJ pointed out that the limitations which, under Directive 2016/680, can be placed on the right to the protection of personal data (Art. 8 CFR), and on the right to respect for private and family life (Art. 7 CFR), must be interpreted in accordance with the requirements of Art.

52(1) CFR, which include respect for the principle of proportionality. Within this framework, the ECJ makes the following key statements:

- The access sought may relate to a very wide range of data (e.g. messages, photos and internet browsing history), and could thus allow very precise conclusions to be drawn concerning the private life of the data subject. In addition, they may include particularly sensitive data. Therefore, such an interference with the fundamental rights to privacy and the protection of personal data must be regarded as serious, or even particularly serious.

- The seriousness of the offence under investigation is an essential parameter when examining the proportionality of the serious interference. However, to consider that only the fight against serious crime may justify access to such data would unduly limit the investigative powers of the competent authorities. This would result in an increased risk of impunity for criminal offences in general and undermine the objective of achieving an area of freedom, security and justice within the European Union.

- That being said, in order to meet the requirement that any limitation on the exercise of a fundamental right must be “provided for by law”, it is for the national legislature to define with sufficient precision the factors, in particular the nature or categories of the offences concerned, which must be taken into account.

- In order to ensure compliance with the principle of proportionality, where access to personal data by the competent national authorities carries the risk of serious, or even particularly serious, interference with the fundamental rights of the data subject, that access must be subject to a prior review carried out by a court or by an independent administrative body.

- This review must take place prior to any attempt to access the data concerned, except in cases of duly justi-

fied urgency, in which case this review must take place within a short time.

- In the context of this review, the court or independent administrative body must be entitled to refuse or restrict an access request falling within the scope of Directive 2016/680 where it finds that the interference with fundamental rights which that access would constitute would be disproportionate.

- Law enforcement authorities must take account of the enhanced level of protection for the processing of sensitive data (as laid down in Art. 10 of Directive 2016/680).

It is now for the referring court to draw the appropriate conclusions from the ECJ’s clarifications. However, given that the interference of the attempts to access personal data on the defendant’s mobile phone was serious and no prior independent authorisation was issued, the Austrian rules seem not compatible with the requirements by the EU law.

➤ *Information rights before data access*

Lastly, the ECJ replied to the question whether CG should have been informed of the attempts to access the data contained in his mobile telephone in order to be able to exercise his right to an effective remedy. In this regard, the ECJ interpreted Art. 13 of Directive 2016/680 (information to be made available or given to the data subject), and, Art. 54 of Directive 2016/680 (right to an effective judicial remedy against a controller or processor) in light of Art. 47 CFR (the fundamental right to an effective remedy and to a fair trial).

According to this legal framework, it is for the competent national authorities which have been authorised by a court or an independent administrative body to access stored data to inform the data subjects of the grounds on which that authorisation is based, as soon as such information is no longer liable to jeopardise the investigations carried out by those authorities.

For the present case this means: Given that CG was aware of the seizure of his mobile phone, informing him of the access attempts would not have harmed the investigation; thus, there were no circumstances that justified a limitation of the right to be informed (Art. 13(3) lit. a) and b) of Directive 2016/680). Hence, CG should have been informed beforehand of the attempts to access the data contained in his mobile telephone.

► *Put in focus*

The ruling in “Landeck” has been considered “[groundbreaking for investigative work](#) and data protection throughout the European Union.” In any case, the judgement is an important contribution to the interpretation of the Law Enforcement Data Protection Directive 2016/680, which is often overshadowed by the General Data Protection Regulation.

The ECJ allows access to cell phone data for all criminal offences, but adds a big “BUT”: Member States must have legislation that respects the proportionality principle. This includes definition of the type or categories of offenses that justify access as well as judicial or independent administrative authorisation *before* police access to the cell phone data to ensure the balance between law enforcement interests and citizens’ fundamental rights. The ECJ also stressed that in urgent cases the authorisation cannot be completely waived but should “take place within a short time”.

The ruling gains importance beyond the legal situation in Austria. EU Member States should scrutinize their national law and potentially adapt it to the parameters set by the judges in Luxembourg.

The “Landeck” case may also prompt national debates for legal reforms. National codes of criminal procedure often do not appear to have been prepared for digitalisation.

In Germany, for example, the rules on search and seizure in the Code of

Criminal Procedure (StPO) do not currently differentiate between complex digital data carriers and other objects. This means that it is currently solely up to the interpretation practice of the public prosecutor’s offices and investigating judges to concretise the principle of proportionality in individual cases. The suspects’ laptops and smartphones are often seized even if the suspicions are tenuous and the vague hope of finding evidence is based solely on experience.

This is why [German lawyers recently called for a change](#) to the existing regulations. Like the ECJ, the majority of the members of the “German Jurists’ Conference” (*Deutscher Juristentag*) rejected the blanket exclusion of the seizure of such devices in the case of minor crimes and misdemeanours. However, they demanded that the law should clarify that the court order authorising the search or seizure must already specify the data to be inspected. The judgement of the ECJ confirms this position – an impulse for the German legislator? (TW) ■

### PNR Agreement with Canada Signed

On 4 October 2024, Commissioner for Migration and Home Affairs, *Ylva Johansson*, and Canadian Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs, *Dominic Leblanc*, [signed a new agreement for the transfer of passenger name records](#) (PNR) data on flights between the EU and Canada. The agreements follows up the CJEU’s decision of 2017 which stopped the conclusion of an EU-Canada PNR Agreement due to its lack of safeguards on data protection, non-discrimination and effective remedy for individuals (→[eucrim 3/2017, 114–115](#)). The new draft aimed to reach compatibility with the requirements set out in the CJEU’s decision and was [finalised in November 2023](#).

[PNR data is](#) personal information provided by passengers and collected and held by air carriers in the context

of their businesses. It includes information such as the name of the passenger, travel dates, itineraries, seats, baggage, contact details and means of payment. The sharing of PNR data is considered useful in preventing, detecting and prosecuting terrorist offences and serious crime.

Before the PNR Agreement with Canada can be concluded, the European Parliament and the Council must give their consent. Once concluded and entered into force, the Agreement will allow Canada and EU Member States to exchange passenger information by air carriers operating between them in a uniform way.

On 29 April 2024, the [European Data Protection Supervisor published an opinion](#) on the deal. He concluded that the draft Agreement contains the necessary safeguards required in order for it to be compatible with the Charter of Fundamental Rights of the European Union. He made, however, several specific recommendations with the aim to ensure that the Agreement would be interpreted and applied in compliance with the CJEU case law. (TW)

### First Periodic Review of the EU–US Data Privacy Framework

On 9 October 2024, the European Commission released a detailed [report evaluating the first periodic review of the EU–US Data Privacy Framework](#) (DPF). The review, carried out in collaboration with European Data Protection Authorities (DPAs), aimed to assess the implementation and operational effectiveness of the framework, which governs the protection of personal data transferred from the European Union to organisations in the United States.

The review took place after the DPF has been in operation for one year. The DPF addresses concerns that personal data leaving EU borders is subject to sweeping US government surveillance (→[eucrim 2/2023, 152–153](#)). It is the meanwhile third attempt to es-

spot  
light

establish legal certainty for data transfers from the EU to the United States after previous such regimes – the EU–US Privacy Shield (2016–2020) and the International Safe Harbor Privacy Principles (2000–2015) – were declared invalid by the European Court of Justice (CJEU) (rulings in *Schrems I* ([→eucrim 3/2015, 85](#)) and *Schrems II* ([→eucrim 2/2020, 98–99](#))).

The Commission's review report acknowledged significant progress made by the United States in implementing the DPF since its adoption. The Commission stated that the United States implemented safeguards to limit access to personal data by US intelligence authorities to what is necessary and proportionate to protect national security. Key developments also included the establishment of a Data Protection Review Court, designed to handle complaints from EU citizens regarding the misuse of their personal data by US entities. This court was recognised as a crucial mechanism for ensuring independent and effective redress. Furthermore, the report noted robust enforcement actions and compliance commitments from participating US organisations, which collectively enhance the framework's credibility and functionality.

Despite these advancements, the review identified areas requiring further refinement to ensure the DPF's effectiveness and its continued alignment with the EU's rigorous data protection standards. Specifically, the Commission pointed out the need for clearer guidance to US organisations to help them fully understand and comply with their obligations under the framework. Additionally, the report called for enhanced oversight mechanisms to proactively monitor adherence to the framework's principles and to address instances of non-compliance more effectively.

The Commission also emphasised the importance of addressing unresolved issues, particularly those related to data access by US public authorities for national security purposes.

While the review highlighted that safeguards had been introduced, such as the principles outlined in Executive Order 14086, the report recommended sustained efforts to ensure transparency, proportionality, and necessity in data access practices.

In its conclusions, the Commission underlined the importance of ongoing dialogue and cooperation between the EU and US to maintain trust in transatlantic data transfers. It reaffirmed its commitment to working closely with US authorities to address the identified gaps and to ensure that the DPF continues to meet the high standards of data protection expected by EU citizens.

Looking ahead, the Commission plans to conduct regular reviews of the framework and to engage with stakeholders, including DPAs, businesses, and civil society, to ensure the DPF evolves in line with technological advancements and emerging privacy challenges. The next review is expected to evaluate the progress made in addressing the recommendations outlined in this initial assessment, with the goal of fostering a reliable and secure transatlantic data transfer environment. (AP)

## Victim Protection

### **ECJ: Compensation to Victims of Violent Intentional Crime Must Be Available to All Family Members**

On 7 November 2024, the ECJ ruled in the preliminary ruling procedure in case [C-126/23 \(Burdene\)](#) that a national scheme that automatically excludes certain family members from a compensation claim as a result of a homicide due to the presence of other family members, without taking into account the circumstances of the individual case, cannot guarantee “fair and appropriate compensation” within the meaning of [Directive 2004/80/EC](#) relating to compensation to crime victims.

### ➤ *Background of the case and legal question*

The case in question is from Italy: A man had killed his former partner and was ordered to pay compensation to the victim's family members. However, he was insolvent, so the Italian state stepped in – but only partially. Under Italian law, a “tiered” compensation scheme was provided for according to the order of succession. For example, under Italian law, in the event of the victim's homicide, the parents would only receive compensation if there was neither a surviving spouse nor children.

The victim's parents, children and siblings then filed a lawsuit, arguing that Italian law no. 122/2016 was incompatible with Art. 12(2) of Directive 2004/80/EC, because the latter stipulates that the amounts of compensation to be paid to victims of violent intentional crime are to be determined “in a fair and appropriate” manner.

### ➤ *ECJ on the applicability of Directive 2004/80*

In its [judgment](#), the ECJ found first that the concept of “victims” pursuant to the Directive must be understood as covering both persons who have themselves been subjected to violent intentional crime, as direct victims, and their close family members where those family members suffer, in turn, the consequences of that crime, as indirect victims.

### ➤ *ECJ on “fair and appropriate compensation” for family members*

Second, the ECJ ruled that the Italian compensation scheme at issue is incompatible with the material concept of Art. 12(2) of Directive 2004/80, which guarantees to Union citizens the right to fair and appropriate compensation for the injuries they suffer on the territory of the Member State in which they find themselves. The ECJ justifies its decision by stating that “a contribution can be regarded as ‘fair and appropriate’ only if it compensates, to an appropriate extent, the suffering to which [the family members] have been exposed.”



Regulations that automatically exclude certain family members from compensation solely on the basis of the presence of other family members, without taking other aspects into account, are to be criticised. In particular, the material consequences for the family members resulting from the death are to be taken into account. The fact that the deceased was responsible for their maintenance or that they lived with them in the same household is also to be considered. (TW)

## Cooperation

### European Arrest Warrant

#### AG Gives Opinion on EAW Competing with Extradition Request

On 5 September 2024, Advocate General (AG) *Nicholas Emiliou* presented his opinion in case [C-763/22 \(Procureur de la République v OP\)](#). The case concerns the conditions under which EU Member States may decide on the competition between a European Arrest Warrant and an extradition request from a non-EU country.

According to AG *Emiliou*, Art. 16(3) of the Framework Decision on the European Arrest Warrant (FD EAW) does not preclude the Spanish regulation whereby a governmental body (the *Consejo de Ministros* [Council of Ministers]) rather than a judicial authority decides on the precedence of a European Arrest Warrant over an extradition request concerning the same person but with different facts underlying the requests. However, such a decision must be subject to judicial review. This follows from Art. 1(3) FD EAW and Art. 47(1) of the Charter of Fundamental Rights of the European Union. Admittedly, the scope of judicial review is limited, namely with regard to the assessment of the precedence criteria set out in Art. 16(3) FD EAW.

The proceedings are based on a request for a preliminary ruling from a French court. That court is conducting criminal proceedings against OP, a French citizen, who is, *inter alia*, prosecuted for counterfeiting payment cards committed in France, Thailand, and Romania. The suspect was arrested in Spain and the Spanish Council of Ministers decided that an extradition request from Switzerland should take precedence over the European Arrest Warrant from France. OP did not agree with this, because he wanted to face the criminal proceedings in France. Apparently, the extradition request from Switzerland and the European Arrest Warrant from France were based on different facts, so that the “Petruhin mechanism” does not apply, as the AG emphasised. (TW)

### Law Enforcement Cooperation

#### German Federal Constitutional Court: Use of EncroChat Data in Criminal Proceedings Admissible

On 1 November 2024, the German [Federal Constitutional Court rejected a constitutional complaint](#) against a criminal conviction for dealing in narcotics in a non-negligible quantity, which was based on the use of EncroChat data as evidence. The complaint was directed against the decision of the Federal Court of Justice (*Bundesgerichtshof*) of 2 March 2022, which in turn confirmed the conviction of the Hamburg Regional Court ([→eucrim 1/2022, 36–37](#)). The Federal Court of Justice explained in detail that German law does not preclude the use of the data that French and Dutch authorities read by infiltrating the EncroChat encryption service in 2020 (for details on the operation [→eucrim 1/2021, 22–23](#)).

► *Background of the case: the 2022 Federal Court of Justice’s decision in EncroChat*

The Federal Court of Justice also approved the procedure whereby the data

collected by the French authorities was transmitted via Europol to the German Federal Criminal Police Office and the Central Office for Combating Internet Crime at the General Public Prosecutor’s Office in Frankfurt am Main had the transmission “subsequently” confirmed by the French investigating judge via a European Investigation Order. The decrypted data, insofar as it concerned users in Germany, was then forwarded to the regionally competent public prosecutors, who then opened and conducted individual criminal proceedings.

► *Inadmissibility of the constitutional complaint*

The Federal Constitutional Court (*Bundesverfassungsgericht*) rejected the constitutional complaint against the conviction as [inadmissible](#), stating that the complaint did not meet the requirements for presentation and substantiation (*Darlegungs- und Substantiierungsvoraussetzungen*). The complainant could not claim a violation of the right to be heard that was relevant to the decision, nor a violation of the guarantee of the lawful judge, nor a violation of fundamental rights. In detail, the Federal Constitutional Court justifies the rejection of the constitutional complaint as follows:

► *No violation of the right to be heard*

The fact that the Hamburg Regional Court did not expressly rule on the defendant’s objection to the use of the EncroChat data does not violate the right to be heard. Moreover, the violation of the right to be heard was remedied by the Federal Court of Justice’s extensively reasoned decision on appeal.

► *No violation of the right to one’s lawful judge*

In the context of the complaint of a violation of the guarantee of the lawful judge, the Federal Constitutional Court deals with the obligation of the German courts to refer the matter to the ECJ. The Federal Constitutional Court agrees with the complainant that the compatibility with EU law (Directive relating to the European In-



investigation Order) was a preliminary question that needed to be clarified and was relevant to the decision on appeal. The Federal Court of Justice should have referred the matter to the ECJ. However, the complainant should have updated his constitutional complaint after the ECJ's decision of 30 April 2024 in Case C-670/22 ([→eucrim 1/2024, 40–43](#)), which concerned the interpretation of the EIO Directive in EncroChat cases. Since he did not do so, he failed to fulfil his obligation to present the case.

But even if the matter were to be taken to court, the violation of the obligation to submit a preliminary reference would be unsuccessful. Indeed, the ECJ does deviate from the Federal Court of Justice to the extent that the judges in Luxembourg demand an examination of whether the transfer of evidence that is already in the possession of the competent authorities of the executing state is only possible if it could have been ordered under the same conditions in a comparable domestic case. The Federal Court of Justice had, however, carried out the ECJ's test incidentally in its ruling: it had referred to an online search pursuant to Sec. 100b of the German Code of Criminal Procedure (StPO), the findings of which were subject to the most restrictive limitation on use under criminal procedure in Sec. 100e(6) StPO. This is not constitutionally objectionable.

► *No violation of privacy right*

Ultimately, the Federal Constitutional Court sees no violation of fundamental rights, in particular the general right of privacy. Insofar as information from the core area of private life is not used, a restriction of the general right of privacy is permissible for the protection of overriding general interests if it is carried out by or on the basis of a law that sufficiently and clearly describes the conditions and scope of the restriction and satisfies the principle of proportionality.

In this context, the Federal Constitutional Court approves the case-law of the ordinary courts: The principle of judge's free evaluation of evidence provided for in Sec. 261 StPO is the constitutional legal basis for the use of evidence in criminal proceedings. In this regard, no special rules apply to the use of evidence that has been introduced into German criminal proceedings from abroad. If information has been obtained unlawfully, there is no constitutional rule that would always prohibit the use of the information obtained. Criminal court practice rightly assumes that the question of whether evidence may be used must be decided in each case according to the circumstances of the individual case. The assumption that evidence may not be used is an exception.

The fact that the Federal Court of Justice assessed the usability according to national law and based its decision on the time of use is just as unobjectionable as the fact that the Federal Court of Justice rejected a violation of

the essential principles of the German legal system by the collection of evidence carried out in France.

► *Put in focus*

The German Federal Constitutional Court rejected the constitutional complaint against EncroChat evidence primarily on formal grounds, but for the first time it has also taken a clear position on the substance. As a result, the case law of the ordinary criminal courts in Germany, the majority of which have ruled against the ineligibility of the data obtained by the French operation using surveillance software against the EncroChat encryption service ([→eucrim 1/2021, 22–23](#)), is not to be criticised. Although further constitutional complaints regarding EncroChat are still pending, the debate in Germany has been possibly ended for the time being. Contrary to many critical voices, the Federal Constitutional Court clarified that the actions of the French investigators did not violate fundamental human and European legal values (TW).



## Council of Europe

*Reported by Thomas Wahl*

### Foundations

#### Artificial Intelligence (AI)

##### Council of Europe Convention on Artificial Intelligence

On 5 September 2024, the first-ever, international, legally-binding instrument on Artificial Intelligence (AI) was [opened for](#)

[signature](#) by the Council of Europe (CoE). The CoE's "[Framework Convention on Artificial Intelligence](#)" provides a common baseline to ensure that activities within the lifecycle of AI systems are fully consistent with human rights, democracy and the rule of law.

Each Party to the Convention is obliged to adopt or maintain appropriate legislative, administrative or other

measures to give effect to the provisions set out in this Convention. These measures shall be graduated and differentiated as may be necessary in view of the severity and probability of the occurrence of adverse impacts on human rights, democracy and the rule of law throughout the lifecycle of AI systems. This may include specific or horizontal measures that apply irrespective of the type of technology used.

➤ *Definition*

The Convention defines “artificial intelligence system” as a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments.

➤ *Territorial Scope*

The Framework Convention on Artificial Intelligence is open to accession to the 46 Council of Europe Member States, the European Union, and states around the world that are not members of the Council of Europe. Involved in elaborating the Convention were for instance the non-member states Argentina, Australia, Canada, Costa Rica, the Holy See, Israel, Japan, Mexico, Peru, the United States of America, and Uruguay. Since the subject of the convention falls within the exclusive competence of the European Union, [only the European Union will become party](#) to the Convention.

➤ *Material scope*

The Convention applies to the use of AI systems in the public sector – including companies acting on its behalf – and in the private sector. Excluded from the scope are:

- Artificial intelligence systems related to the protection of a Party’s national security interests (but the Party will be obliged to ensure that AI activities respect international law and democratic institutions and processes);
- Research and development activities, except when the testing of AI systems or similar activities may have

the potential to interfere with human rights, democracy or the rule of law;

- Matters relating to national defence.

➤ *Main obligations*

The Framework Convention sets forth general obligations and common principles that each Party is obliged to implement in regard to AI systems. Parties must ensure, for instance, that the activities within the lifecycle of AI systems are consistent with obligations to protect human rights, as enshrined in applicable international law and in their domestic law. They must also adopt or maintain measures that protect the integrity, independence and effectiveness of democratic institutions and processes.

The Convention establishes transparency and oversight requirements tailored to specific contexts and risks, including identifying content generated by AI systems. Parties must adopt measures to identify, assess, prevent, and mitigate possible risks and assess the need for a moratorium, a ban or other appropriate measures concerning uses of AI systems where their risks may be incompatible with human rights standards.

Parties are also obliged to ensure accountability and responsibility for adverse impacts and that AI systems respect equality, including gender equality, the prohibition of discrimination, and privacy rights.

Other provisions of the Convention relate to topics such as public consultation and digital literacy/skills.

➤ *Remedies and safeguards*

The Convention sets the parameters for accessible and effective remedies for violations of human rights resulting from the activities within the lifecycle of AI systems. It is considered important, for instance, that the relevant content in the information-related measures should be context-appropriate, sufficiently clear and meaningful, and critically, provide a person concerned with an effective ability to use the information in question to exercise

their rights in the proceedings in respect of the relevant decisions affecting their human rights.

Procedural safeguards must include that persons interacting with AI systems are notified that they are interacting with such systems rather than with a human.

➤ *Risk assessments*

Similar as the EU legislation (for the EU AI Act → [eucrim 4/2023, 316–317](#)), the CoE Convention follows a risk-based approach. The Convention introduces minimum requirements for risk assessments: Parties are obliged to identify, assess, prevent and mitigate ex ante and, as appropriate, iteratively throughout the lifecycle of the AI system the relevant risks and potential impacts to human rights, democracy and the rule of law by following and enabling the development of a methodology with concrete and objective criteria for such assessments. These obligations are key to enable the implementation of all relevant principles, including the principles of transparency and oversight as well as the principle of accountability and responsibility.

The Convention also provides that, in the risk and impact assessment process, attention should be paid both to the dynamic and changing character of activities within the lifecycle of AI systems and to the shifting conditions of the real-world environments in which systems are intended to be deployed. Requirements are introduced regarding not only the documentation of the relevant information during the risk management processes, but also the application of sufficient preventive and mitigating measures in respect of the risks and impacts identified.

➤ *Follow-up*

In order to ensure its effective implementation, the Convention establishes a follow-up mechanism in the form of a “Conference of the Parties”, composed of representatives of the Parties. In addition, each Party will be obliged to provide a report to the Conference of the

Parties within the first two years after becoming a Party and then periodically thereafter with details of the activities undertaken to give effect to the use of AI systems in the public and private sector. Last but not least, Parties are required to adopt or maintain effective mechanisms to oversee compliance with the obligations in the Framework Convention. Oversight bodies must be functionally independent from the relevant actors within the executive and legislative branches.

► *Background*

Negotiations on the Convention began back in September 2022 under the auspices of the [Committee on Artificial Intelligence \(CAI\)](#) established by the Council of Europe in Strasbourg. The negotiating process not only brought together government representatives from the Council of Europe member states and non-member states (see above), and from the European Commission (negotiating on behalf of the European Union), but also representatives from civil society, academia, industry, and other international organisations who participated as observers.

On 5 September 2024, the Convention was [signed by 10 states](#) (including Israel and the United States of America as non-member states of the Council of Europe) and by the European Commission on behalf of the European Union.

The Convention will enter into force after five states have given their consent to be bound by the Convention (e.g. after ratification); at least three out of these five states must be member states of the Council of Europe.

For the EU, the Convention means that it will be implemented by means of the EU AI Act which entered into force on 1 August 2024 and contains generally fully harmonised rules for the placing on the market, putting into service and use of AI systems in the EU (→ [eucrim 2/2024, 92–93](#)).

*Eucrim* will regularly update the accessions to the Framework Convention

on Artificial Intelligence (CETS No. 225) on its [website documenting ratifications](#) of CoE Conventions. ■

### Council of Europe Recommendation on Artificial Intelligence in Prisons and Probation

On 9 October 2024, the Council of Europe's Committee of Ministers issued a new [Recommendation](#) regarding the ethical and organisational aspects of the use of artificial intelligence and related digital technologies by prison and probation services.

The [Recommendation aims to](#) establish principles and rules that guide the Council of Europe member states in their legislation, criminal policy and practice, given that the use of artificial intelligence (AI) for criminal justice purposes is advancing at great pace and execution of penal sanctions and measures is one of strongest manifestations of public power that deeply interferes with human dignity, human rights and privacy, including the collection and processing of personal data.

As a guiding principle, the Recommendation stresses that prison and probation services use AI and related digital technologies legitimately and proportionately and only if they contribute to the rehabilitation of offenders. AI and related digital technologies should not replace prison and probation staff but rather assist them in their everyday work, and help the criminal justice system, the execution of penal sanctions and measures and the reduction of recidivism.

The Recommendation defines first nine basic principles if AI and related digital technologies are designed, developed, provided, used and decommissioned. These principles are, for example, the principle of legality, legal certainty and liability, the principle of good governance, transparency, traceability and explicability, the principle of the right to a human review of decision, and the principle of human-centred use of AI and related digital technologies.

Next to data protection and privacy issues, the Recommendation deals with various use scenarios of AI in the context of prisons and probation services, such as:

- Use for the purpose of safety, security and good order;
- Use for offender management, risk assessment, rehabilitation and reintegration;
- Use for staff selection, management, training and development.

The Recommendation sets out for instance that the use of AI for maintaining safety, security and good order can be for the benefit of better risk and crisis management, but should be strictly necessary, proportionate to the purpose and avoid any negative effects on the privacy and well-being of offenders and staff.

Looking at the use of AI vis-à-vis offenders, the Recommendation makes the point that rehabilitation and reintegration of offenders, as well as their social contacts, may be facilitated by the use of AI and related digital technologies. When such tools are used for the personalisation of treatment and reintegration plans, this should be done with care to avoid biases. The use of such tools should not replace regular face-to-face human contact between professionals and the offenders, including, where necessary, the work with their families and children.

AI should also be applied with care if it comes to its use for managing appointments and interventions (including appointments with healthcare professionals, lawyers, social workers and any other professionals).

*Background:* As a sector-specific work, the Recommendation complements the Council of Europe's more general Framework Convention on Artificial Intelligence which was opened for signature on 5 September 2024 (→ *supra* pp. 194 et seq.). The Framework Convention is a first-of-its-kind global legally binding instrument designed to ensure that AI upholds

common standards in human rights, democracy and the rule of law, and to minimise the risk of those rights and principles being undermined as a result of the use of AI.

The Council of Europe has also published a [brochure](#) in which it provides information on its efforts to promote the establishment of standards that meet the challenges to human rights posed by the use of AI systems.

## Human Rights Issues

### New Misuse of Power Factsheet

On 14 November 2024, the Council of Europe published [a new factsheet summarising the ECtHR's case law on Article 18 ECHR](#), which limits the use of restriction on human rights guaranteed in the Convention. Article 18 ECHR ensuring that restrictions on rights and freedoms are applied only for purposes authorised by the Convention itself. It thus plays a central role in preventing the misuse of power by states. Article 18 ECHR is rarely invoked and the ECtHR found violation of this article rarely. However, if violations take place, the provision can have important effects, such as for the award of compensations by national authorities and legal reforms to strengthen the independence of the judiciary.

## Institutions

### European Committee on Crime Problems (CDPC)

#### 86th CDPC Plenary Meeting: Advancements in Various Crime Areas

At its [86th Plenary meeting](#), the European Committee on Crime Problems (CDPC) took important decisions on the advancement of cooperation and prevention in criminal matters. The [CDPC](#) is the Council of Europe's steer-

ing committee responsible for overseeing and coordinating the Council of Europe's activities in the field of crime prevention and crime control. It identifies priorities for intergovernmental criminal law co-operation, and implements activities in the fields of criminal law and procedure, criminology and penology. Two subordinate committees assist the CDPC: the Committee of experts on the operation of European conventions on co-operation in criminal matters (PC-OC) and the Council for penological co-operation (PC-CP).

At its 86th Plenary meeting from 20 to 22 November 2024, [the CDPC, \*inter alia\*, achieved results](#) in the following areas:

- Approval of the draft Convention on the Protection of the Environment through Criminal Law and its Explanatory Report: The Convention is set to be the first legally binding instrument with global impact to address environmental crime. The Convention will allow tackling a wide range of criminal acts detrimental to the environment, such as pollution, hazardous waste, illegal logging, trading in wildlife species, mining and the disruption of protected habitats. The draft Convention is transmitted to the Council of Ministers for adoption and it is expected that the Convention will be opened for signature in May 2025.

- Approval of the draft Third Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters and its Explanatory Report: The Protocol will modernise the existing, multilateral provisions governing mutual assistance, extend the range of circumstances in which mutual assistance may be requested, facilitate assistance and making it quicker and more flexible. Hence, the Third Additional Protocol would establish electronic communications as the preferred channel of communication, promote hearings by video-conference, set up a framework of cooperation for

the use of technical recording devices in the territory of another party, and facilitate the cross-border interception of telecommunications.

- Approval of the draft Recommendation on the promotion of positive mental health and the management of mental disorders of prisoners and probationers. It was decided that the draft text (together with the Explanatory Memorandum) is forwarded to the Council of Ministers for adoption.

- Start of work on drafting a new recommendation on migrant smuggling. The CDPC also examined activities and advancements in a number of other areas, including: combating technology-facilitated violence against women and girls, artificial intelligence and criminal law, asset recovery, combating organised crime related to drug trafficking, hate crime, restorative justice, and the Council of Europe Conventions on offences relating to Cultural Property, Medicrime and Trafficking in Human Organs.

## Specific Areas of Crime

### Corruption

#### GRECO Concerned About Corruption Situation in Slovakia

After a high-level visit to Slovakia on 26 September 2024, [GRECO voiced concerns over](#) the lack of process in the country's fight against corruption. GRECO stated that Slovakia has largely not complied with GRECO's recommendations from the 5th evaluation round addressing the prevention of corruption and strengthened integrity within the central government (persons with top executive functions) and the police force.

GRECO noted that six years after the adoption of its evaluation report on the Slovak Republic, only three out of 21 recommendations have been implemented in full. GRECO will monitor

the Slovak authorities' progress in implementing its recommendations at its Plenary meeting in 2025 based on information to be provided by the Slovak authorities at the end of 2024.

### GRECO: Fifth Round Evaluation Report on Italy

On 28 August 2024, GRECO published its [5th Round Evaluation Report on Italy](#). The report addressed the effectiveness of the framework in place in Italy as regards the prevention of corruption among persons with top executive functions (PTEFs), and corruption prevention in law enforcement authorities, including the Italian State Police, the Carabinieri and the Guardia di Finanza.

GRECO acknowledged that Italy has a sizeable legal and institutional framework dealing with the prevention and fight against corruption. However, this framework is complicated to navigate, to the detriment of its efficiency. An example is the regulation of conflicts of interest, where several texts address different aspects of such conflicts for different categories of officials. Conversely, ministers' advisers are not covered by any of these regimes. Deficiencies also exist with regard to financial disclosure regimes for ministers and their advisers.

Improvements are needed with regard to integrity checks of PTEFs. These improvements should include, for instance:

- Carrying out, on a regular basis, a systemic analysis of corruption and integrity-related risks covering all PTEFs;
- Adopting code(s) of conduct for PTEFs, which are (1) complemented with clear guidance regarding conflicts of interest and other integrity-related matters (such as gifts, contacts with third parties, outside activities, contracts with state authorities, the handling of confidential information and post-employment restrictions), and (2) coupled with a credible and effective mechanism of supervision and sanctions;

- Developing efficient internal mechanisms to promote and raise awareness of integrity matters in the government.

GRECO noted that Italy made progress in setting up transparency rules. Further measures should ensure an appropriate level of general public consultation on government draft legislation. More light should also be shed on the contacts of PTEFs with lobbyists.

Looking at the area of law enforcement, GRECO criticised the low representation of women in the State Police, the Carabinieri and the Guardia di Finanza, especially at managerial level. Although all three forces have a robust system in place for the prevention and management of integrity risks, GRECO makes a number of recommendations for improvements:

- The State Police needs a dedicated code of conduct, accompanied by effective oversight and enforcement;
- The Carabinieri and the Guardia di Finanza need to complement their ethical rules by more practical guidance;
- It holds true for all three forces that mechanisms for confidential counselling on integrity matters be introduced;
- Integrity checks should be carried out in case of transfers of staff and promotions.

Lastly, GRECO recommends increasing training and awareness-raising activities on whistleblower protection measures in the law enforcement authorities.

GRECO invited Italy to submit a report on the measures taken to implement GRECO's recommendations by the end of September 2025. GRECO will monitor compliance with the recommendations in 2026.

### Money Laundering

#### MONEYVAL: Annual Report for 2023

In its [annual report for 2023](#), published on 8 November 2024, MONEYVAL provides an overview of compliance trends of in the states and jurisdic-

tions which have been evaluated as regards their compliance with international standards on combatting money laundering, the funding of terrorism and of the proliferation of weapons of mass destruction.

The report positively highlighted that MONEYVAL member states and jurisdictions are making progress in certain areas, such as their understanding of money laundering and terrorist financing risks, international cooperation and the use of financial intelligence. In addition, countries have comprehensive legal frameworks and powers to prosecute money laundering.

MONEYVAL sees, however, room for improvements in the supervision of the financial sector, private sector compliance, transparency of legal persons, and the implementation of targeted sanctions for the financing of terrorism and the proliferation of weapons of mass destruction. Many countries struggle to achieve positive results in prosecuting and convicting perpetrators. The confiscation of criminal assets remains an area for concern because only modest results have been achieved.

Looking at MONEYVAL's key activities in 2023, the report stressed that MONEYVAL nearly completed the fifth round of mutual evaluations. The last two reports (on Bosnia-Herzegovina and the UK Crown Dependency of Guernsey) will be finalised in December 2024. By the end of 2023, 20 of the 33 states and territories evaluated by MONEYVAL in the fifth round of mutual evaluations were subject to its enhanced follow-up procedure for their limited level of compliance with anti-money laundering and counter-terrorist financing standards. The report also pointed out that MONEYVAL started the sixth round of mutual evaluations with an on-site visit to Latvia. The first report of the sixth evaluation round (on Latvia) is scheduled for June 2025.



In this context, [Nicola Muccioli, Chair of MONEVVAL](#), said: “The launch of MONEVVAL’s 6th evaluation round will allow us to strengthen further the focus on monitoring the real effectiveness of the legal frameworks in place to combat the major risks of money laundering and terrorist financing. We can only make progress in fighting these crimes if the legislation and practices are implemented in practice.”

## Procedural Law

### European Commission for the efficiency of justice (CEPEJ)

#### CEPEJ: 2024 Report on European Judicial Systems

**spot light** On 16 October 2024, the European Commission for the Efficiency of Justice (CEPEJ) published the [tenth biennial evaluation report on European judicial systems](#). The report is based on data from 2022 and provides tools for a better understanding of the functioning of justice in the CoE member states and some observers states, in order to improve efficiency and quality of justice in the interest of close to 700 million Europeans. It also supports the prevention of violations of Article 6 ECHR. The tenth evaluation cycle analysed the judicial systems of 44 CoE member states (Liechtenstein and San Marino did not provide data) as well as Israel and Morocco as observer states.

The report has three parts:

- [Country profiles](#) summarising key data and indicators for each evaluated country;
  - [CEPEJ-STAT](#), an online database containing CEPEJ data since 2010, and making available to policymakers, legal professionals, and researchers various dashboards as a result of which comparisons between states with sound data can be made. CEPEJ also pointed out that this is the first edition of the report using post-COVID data, the pandemic having also affected the functioning of justice in Europe ([→ eucrim 3/2022, 201–202](#) for the 2022 report). The key findings of the 2024 evaluation report are as follows:
    - *Budget allocated to justice systems*
      - Budgets allocated to the judicial system remain relatively small compared to other public sectors and the judiciary’s significance: European countries spent on average €85,4 per inhabitant (7,31 € more than in 2020) and 0,31% of GDP on their judicial systems;
      - On average, member states and entities spent about 2/3 of their judicial system budget on courts, around 25% on public prosecution services and the remaining on legal aid (11%);
      - On average, there has been a notable 16% decrease in spending on legal aid since 2020.
    - *Justice professionals*
      - In 2022, Europe had an average of 22 judges per 100,000 inhabitants (from a minimum of 3 judges per 100,000 inhabitants in England and Wales to a maximum of 42,4 in Croatia and Montenegro);
      - On average, there were 12 prosecutors per 100,000 inhabitants (also here, there are great variations ranging from 3 prosecutors per 100,000 inhabitants in France and Ireland to 24 in Bulgaria, Latvia, and Moldova);
      - There was an average of 180 lawyers per 100,000 inhabitants (from 23 in Azerbaijan to 505 in Cyprus);
      - There were more women judges and prosecutors than men in Europe
- (57% of the professional judges and 54% of the public prosecutors are female), but the glass ceiling, i.e., the underrepresentation of women in the highest positions, is still present;
- Only in 28% of states, public prosecutors are subject to a ban of instructions – an important element for their independence;
  - Between 2012 and 2022, the salaries of judges and public prosecutors as a proportion of average salaries increased slightly in Europe, although there were significant disparities, with some countries seeing decreases.
- *Access to justice*
    - 44 states and entities provide free online access to legal texts, higher courts jurisprudence, and other various information about the judicial system through their courts’ websites;
    - Only in 3 member states access to court is free of charge;
    - Legal aid is available in all evaluated countries for criminal, civil and administrative cases, regularly following an evaluation of the applicant’s income and assets;
    - In some countries, specific categories of persons, e.g. victims of domestic or sexual violence, immigrants or asylum seekers, are automatically granted legal aid;
    - The downward trend in the number of courts in Europe has been confirmed in 2022;
    - In 2022, the existence of alternative mechanisms to resolve disputes, as well as digital solutions appear more and more as a mean to enhance access to justice;
    - In over 70% of countries digital tools are available to file a case or communicate with the court, but the real usage in the field of justice is low.
  - *Efficiency and quality*
    - Compared to 2020 data, which were largely affected by the COVID-19 pandemic, figures for 2022 indicate that the European justice systems improved in terms of efficiency, but the pre-pandemic level has largely not been reached;

- The situation of efficiency depends on the type of case (civil, criminal, administrative) and the level of jurisdiction (first, second, Supreme Court). For example, while criminal cases have seen a reduction in processing times at first instance, the length of proceedings increased in first and second instances for civil and commercial cases;

- Administrative justice was the least efficient;

- Third-instance courts were the most efficient in all case types;

- Problems with prosecutorial efficiency have persisted over time. Looking at the clearance rate, the prosecutorial efficiency remains a challenge across Europe.

➤ *Information and communication technologies (ICT)*

- Investment in ICT is constant and almost all states have increased their average ICT budget per inhabitant;

- The deployment of ICT tools varies across different matters and countries, with the civil matter often exhibiting higher adoption levels compared to administrative and criminal matters;

- Since the last cycle and after COVID, many states and entities have made notable progress in introducing remote hearings in courts and in 33 states this is possible in criminal matters;

- The evaluation cycle saw the start of new innovative AI tools to assist judges, which became particularly relevant for areas such as class actions, automatic anonymisation of judgments, and specialised translation;

- When countries are grouped by their

level of digitalisation, a pattern seems to emerge, suggesting that higher ICT deployment is associated with lower case processing times.

In the context of ICT, the CEPEJ report also pointed out that states must better distinguish between deployment and usage data. Many judiciaries must still make the effort to collect the data needed to assess and steer their e-justice initiatives. Implementing robust mechanisms to track and evaluate the utilisation rates of ICT tools within the justice domain is considered crucial not only to improve resource allocation but also to ensure transparency and accountability. ■

### **Consultative Council of European Public Prosecutors (CCPE)**

#### **CCPE: Opinion on Strengthening Independence of Prosecution Services**

On 29 October 2024, the Council of Europe's Consultative Council of European Prosecutors (CCPE) published an [Opinion on managing prosecution services to ensure their independence and impartiality](#). The Opinion also aims at reinforcing the efficiency of the work of prosecution services.

Given that prosecution services in most European countries have a hierarchical structure, led by a prosecutor general, the Opinion focuses on the central role played by prosecutors general as guarantors of prosecutorial independence through

the management of prosecution services.

Taking into account the work by other CoE bodies and institutions, the CCPE developed several principles for independence and impartiality for the following aspects:

- The appointment/election procedure, in addition to the term of office of prosecutors general, the safeguards concerning their removal and against undue interference with their work; Ethical and professional standards, accountability and disciplinary proceedings;

- The management functions of prosecutors general and their tasks, in particular with regard to careers of prosecutors and staff of the prosecution services, and consistent application of law and case management.

The CCPE agreed on 16 recommendations that are to ensure full independence and impartiality of prosecutors general. They include that influence of the executive on prosecutors' general appointment or election must be prevented, clear and objective criteria for their selection must be determined, clear rules and procedures for disciplinary proceedings must be established, there must be guarantees regarding any possibility of removing them from office before the end of their term, and relationships between the different layers of the hierarchy in the prosecution services must be governed by clear and unambiguous rules so that personal or other considerations do not play an unwarranted role.

# Articles

## Articles / Aufsätze

Fil Rouge

Over the past few years, the European Union and international law have seen a surge of new regulations governing artificial intelligence (AI) and digitalisation. In his guest editorial, *Jorge Espina* already guided us through this parcours of legislation. AI and digitalisation offer manifold opportunities but also entail multiple challenges, which are explored in the articles in this issue of *eu-crim*. They focus on the impact of new technologies on justice in the broader sense, bringing to the fore the overall theme: “The Digitalisation of Justice”.

*Iona Mazilescu* and *Katerina Entcheva* introduce the article section by explaining the main elements of the two recent pieces of EU legislation with high relevance for the justice sector: the AI Act (Regulation (EU) 2024/1689) and the Regulation on the digitalisation of judicial cooperation (Regulation (EU) 2023/2844). The authors also outline the anticipated benefits of enhancing the quality of justice by means of this new regulatory framework.

The second section of the issue provides insights into the use of digital tools in investigative practice:

- *Georg Roebing* and *Bogdan Necula* reflect on the potential use of large language models and other artificial intelligence-based software to support anti-fraud investigations. They shed light on the practical challenges and limitations as well as legal restrictions that follow from the AI Act and European data protection rules.
- In turn, *Boudewijn de Jonge* and *Barry de Vries* illustrate the Dutch experience with data-driven police investigations and their ensuing challenges. They also reveal the practical police work involved in meeting the requirements of data protection (the Law Enforcement Directive) and lay out the preconditions for successful international cooperation on large data sets, which were able to be derived from cases such as *EncroChat* and *SkyEEC*.

The third section addresses the impact of digitalisation on procedural safeguards and fundamental rights. These articles identify legal gaps and call for European legislative action:

- *Lorena Bachmaier Winter* explores standards for the lawyer-client privilege in EU cross-border criminal proceedings in light of advancing digitalisation. Taking the case law of the European Court of Human Rights

as a starting point, she argues that there is a need for the European Union to take legislative action in order to ensure the effective protection of the right to confidentiality of lawyer-client communications.

- Closely related to the lawyer-client privilege (and even a decisive step ahead) is the right to access to a lawyer. *Tomohiro Nakane* discusses access to a lawyer via videoconferencing for detained suspects and accused persons. He analyses the legal situation in Germany, demonstrates the benefits of access to a lawyer via videoconferencing tools, and ultimately pleads for a revision of the underlying Union law, i.e., Directive 2013/48.
- *Judit Szabó* and *Dominik Brodowski* continue the discussion on the use of videoconferencing technology by examining the current legal possibilities to hold “virtual trials” through videoconference in transnational situations in the EU. Taking into account the reference for a preliminary ruling in the Joined Cases C-255/23 (*AVVA and Others*) and C-285/23 (*Linte*) at the CJEU, the authors provide examples of the Hungarian and the German criminal justice systems. Based on their analysis, *Szabó* and *Brodowski* conclude that the question of transnational virtual criminal trials should be addressed by the European legislature.

The last article is at the crossroads between fundamental rights protection and the extent of regulation of online platforms – a topic that is currently being hotly debated. *Randall Stephenson* and *Johanna Rinceanu* follow up on their earlier article “Differential Iatrogenesis” (*eu-crim* 1/2023, 73–82) and explore which model should be used to tackle “problematic” online content (e.g., hate speech and misinformation). In their in-depth analysis of Canada’s “systems-based” approach, the authors argue that censorship concerns may yet necessitate reassessment of Europe’s current regulatory framework.

The potential benefits and risks surrounding AI and digitalization will continue to require close monitoring as these technologies advance at lightning speed.

*Thomas Wahl*, Senior Researcher at Max Planck Institute for the Study of Crime, Security and Law & Managing Editor of *eu-crim*

# Artificial Intelligence and Digitalisation of Judicial Cooperation

## The Main Provisions in Recent EU Legislation

Ioana Mazilescu and Katerina Entcheva\*

Artificial intelligence (AI) tools are increasingly being used by justice professionals to improve the speed and the efficiency of legal proceedings and to alleviate administrative burdens. Digital and AI tools may be a game changer in enhancing the quality of justice and allowing justice professionals to concentrate on more substantive tasks. Digitalisation and the use of AI in justice bring about significant benefits but can also present certain risks, thus requiring a clear regulatory framework. The last few years have brought about a considerable number of new rules agreed at EU level that cover different aspects of the digital developments experienced by our society and economy.

This article presents the main elements of two of these acts: the AI Act and the Regulation on digitalisation of judicial cooperation, focusing on the aspects with the most relevance for the justice sector. It explains which AI practices are prohibited and the approach to regulating AI systems. It then presents the digital technology tools that will underpin cross-border cooperation between judicial authorities in the EU and will help citizens to access courts more easily and conveniently in cross-border disputes. In a nutshell, the article explains the regulatory framework and the expected benefits of digitalising judicial cooperation and access to justice. The next steps related to these laws are also briefly explained, and the authors conclude that further digitalisation in the justice field is to be expected.

## I. The Artificial Intelligence Act

### 1. Introductory Remarks

As announced in its White Paper on Artificial Intelligence (AI) of 2020,<sup>1</sup> the European Commission has proposed several pieces of legislation aimed at creating an ecosystem of trust to facilitate the uptake of AI in the European Union. Several of these proposals have amended particularly the EU acquis concerned with the safety of products. In this context, the Commission had proposed a legislative package on liability in 2022: the proposals for the AI Liability Directive (AILD)<sup>2</sup> and the revision of the Product Liability Directive (PLD)<sup>3</sup>. Against this background, this article will focus on describing the provisions of the main legal framework regulating AI systems in the EU: The Artificial Intelligence Act (Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence).<sup>4</sup>

### 2. Key provisions of the AI Act particularly in relation to the justice sector

Regulation 2024/1689 entered into force on 1 August 2024. The AI Act provides for fully harmonised rules for the following:

- Placing on the market, the putting into service, and the use of AI systems in the European Union;
- Prohibitions of certain AI practices;

- Specific requirements for high-risk AI systems and obligations for operators of such systems;
- Certain transparency rules;
- Rules on market surveillance and enforcement.

The Regulation stipulates **clear requirements and obligations for AI developers and deployers** regarding specific uses of AI. At the same time, the regulation seeks to reduce administrative and financial burdens for business, in particular small and medium-sized enterprises (SMEs). The AI Act follows a **risk-based approach**, i.e., some AI practices are prohibited and some are considered high-risk and are subject to specific requirements; certain transparency rules are applicable to specific situations. Yet, AI systems that do not fall under the categories or uses regulated in the AI Act can be developed and placed on the EU market without being subject to any specific rules. Certain AI tools for the administration of justice are classified as high-risk; therefore, they have to comply with specific requirements.

The AI Act aims to ensure that when AI is used, including in the justice sector and the administration of justice, safeguards and control mechanisms are in place to minimise risks to fundamental rights, safety, and the rule of law, among others.



The legal framework set out by the AI Act follows the objective of boosting the trustworthy use of AI tools across sectors, including in the area of justice. In turn, this would contribute to supporting judges and justice professionals in the administration of justice and to improving the efficiency of judicial procedures. However, national judicial authorities preserve the right to opt for or against the use of AI in the justice sector.

### Prohibited AI practices

Overall, the AI Act recognises that certain AI systems are considered too risky and thus **prohibited by law**. For example, in the context of AI in the area of justice, the act bans the placing on the market, the putting into service, or the use of an AI system for making risk assessments of individuals in order to assess or predict the risk of committing a criminal offence, based solely on the profiling of this person or on assessing their personality traits and characteristics. The Commission has been tasked with adopting guidelines for the practical implementation of this provision by February 2025.

### High-risk AI systems

In addition, the AI Act classifies **certain AI systems used in specific areas as high-risk**. Putting on the market and use of such systems will be subject to strict obligations for both the entities developing them and their deployers (i.e., legal persons or professionals who use AI systems). Additional obligations and requirements for deployers may apply to fulfil EU or national obligations, for instance in the area of consumer law, product liability, and data protection.

AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts are one example of what is considered high-risk AI systems. This is due to their potentially significant impact on the rule of law and on the fundamental rights enshrined in the Charter of Fundamental Rights of the EU, notably the right to a fair trial and to an effective remedy, the presumption of innocence and the right of defence, human dignity, and non-discrimination.

The AI Act therefore recognises and reaffirms the **role of the judge**: while the use of AI tools can support the judiciary, it should not replace the decision-making power of judges. The final decision-making must remain a human-driven activity.

Moreover, the following AI systems are considered high-risk and consequently subject to the requirements explained above:

- AI systems intended to be used by law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups,<sup>5</sup> and
- AI systems intended to be used for the profiling of natural persons in the course of the detection, investigation, or prosecution of criminal offences.

### Non-high risks AI systems

At the same time, AI systems for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases are not considered high-risk. This may concern, for example: a) the anonymisation or pseudonymisation of judicial decisions, documents or data, b) communication between personnel, or c) administrative tasks.

### Derogations

The AI Act establishes a derogation for the use of certain high-risk AI systems, which is relevant for the use of AI in the area of justice. Such systems should not pose a significant risk of harm to the fundamental rights of individuals, e.g., by not materially influencing the outcome of decision-making. The derogation applies where one of the following conditions is fulfilled:

- The AI system is intended to perform a narrow procedural task;
- The AI system is intended to improve the result of a previously completed human activity;
- The AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review, or;
- The AI system is intended to perform a preparatory task to an assessment relevant, for instance, for AI in justice.

To guide the application and interpretation of the AI Act in general, including the use of AI in the administration of justice, the AI Act empowers the European Commission with issuing guidance in respect of prohibited practices (by February 2025) and of high-risk AI systems (by February 2026).

This guidance will be particularly relevant for those **Member States already using AI** or intending to do so in the justice sector. From the current information available from a

number of EU Member States, a range of projects using AI in justice is being developed or starting to be used at national level. In 2023, five Member States were planning to use AI in their justice systems, while in six Member States courts and prosecutors use some AI applications in core activities.<sup>6</sup>

## II. The Digitalisation Regulation

### 1. Introductory Remarks

Regulation (EU) 2023/2844 (hereinafter Digitalisation Regulation)<sup>7</sup> aims to improve the efficiency and the resilience of cross-border judicial cooperation procedures, still mostly a paper-based endeavour as things stand. It will also enhance access to justice, as citizens and companies will have the option of using digital communication channels to make certain submissions to the competent authorities and to participate remotely in court hearings through videoconferencing and other distance communication technologies.

### 2. Key elements

The Digitalisation Regulation provides a comprehensive legal framework for the use of digital technologies in **civil, commercial, and criminal cases with cross-border implications** by establishing rules on digital communication between competent judicial authorities, and between natural and legal persons (parties to the proceedings) and the competent judicial authorities. It is also applicable to electronic exchanges with Union agencies and bodies. Additionally, the Regulation establishes a legal basis for conducting videoconferencing sessions across Member States and lays down harmonised rules on the acceptance of electronic documents and electronic signatures and seals, building up synergies with the eIDAS Regulation<sup>8</sup>. The Digitalisation Regulation includes the following main elements:

- **The use of an e-CODEX-based decentralised IT system** is mandatory for digital exchanges between competent judicial authorities and between these authorities and the Union agencies and bodies. This obligation is subject to certain limited and well-defined exceptions where the use of the decentralised IT system is either not possible (e.g., disruption of the system, physical nature of the material, etc.) or not appropriate (e.g., direct judge-to-judge communication, etc.);
- **The use of digital communication channels** by natural and legal persons is optional and applies only in civil and

commercial matters. The Regulation establishes a European electronic access point (EEAP) on the e-Justice Portal, which would allow natural and legal persons to submit cases or otherwise communicate with the competent authorities;

- The Regulation allows for the use of **videoconferencing and other distance communication technology** in the following ways:
  - In **civil and commercial matters** – the provision applies where at least one of the parties to the proceedings or their representative is present in the territory of another Member State. The possibility is subject to the discretion of the authority – the decision should be based on the existence of the technology, the opinion of the other party, and the appropriateness of the use of such technology for the purposes of the case at hand. The procedure for holding the hearing should be the one under the applicable national law;
  - In **criminal matters**, the scope of videoconferencing is limited to certain judicial cooperation procedures. Special attention is paid to the protection of the procedural rights of the persons. Again, national law governs the procedure for conducting videoconferencing;
- **Qualified electronic signatures/seals** must be used for communication between competent authorities and between these authorities and the Union agencies and bodies. Natural or legal persons may either use a qualified electronic signature or seal, or electronic identification with assurance level high, as specified in the eIDAS Regulation;
- Documents **should not be denied legal effect** only because they are in electronic form;
- **Training** of justice professionals should be ensured by Member States.

The Regulation is complemented by some technical provisions:

- The decentralised IT system will be established by implementing acts. 24 implementing acts in total will be adopted by 2028. The adoption of each implementing act will be followed by an implementation period of two years for the actual development of the reference implementation software (or national back-end system) and deployment of the system at national level;
- The Commission will provide a reference implementation software, which Member States may select over nationally developed back-end systems.
- The Commission will set up and maintain the EEAP and will provide for user support.

The Regulation entered into force on 16 January 2024. The **date of application** will be 15 months from the entry into force of the regulation for the videoconferencing provisions and two years from the date of entry into force of the corresponding implementing acts setting up the decentralised IT system and EEAP.

The work on the implementing acts is currently underway with discussions on the first batch of implementing acts. In criminal matters, the procedures relating to the European Investigation Order, the European Arrest Warrant, and the Freezing and Confiscation Orders will be the first ones to be digitalised.

### III. Final remarks

The digitalisation of justice is clearly an ongoing process that will continue. It will require a combination of measures, from funding and organisational aspects, to rule setting and training. Digitalisation implies, on the one hand, specific measures at the level of each institution and, on the other hand, coordinated efforts at national and European level to respond to the needs of justice in the most efficient way. Digitalisation is a necessary and inevitable process that should lead to more accessible, transparent, and efficient justice and which responds to the demands and expectations of our increasing digitalised economy and society.

\* The information and views set out in this article are those of the authors and do not necessarily reflect the official opinion of the European Commission.

1 White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, available at: <[https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust\\_en](https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en)> accessed 10. January 2025.

2 Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final.

3 Proposal for a Directive of the European Parliament and the Council on liability of defective products, COM(2022), 495 final.

4 Full reference: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

5 As mentioned above under “prohibited AI practices”, risk assessments concerning an individual in order to assess the likelihood of their committing a crime or predicting the occurrence of an actual or potential crime based solely on profiling an individual or on assessing their personality traits and characteristics is prohibited. In line with the presumption of innocence, individuals should always be judged on their actual behaviour, thus such tools should only support a risk assessment when there are objective, verifiable facts to support a reasonable suspicion and if there is a human assessment.

6 The 2024 EU Justice Scoreboard, COM(2024) 950, available at: <[https://commission.europa.eu/document/download/84aa3726-82d7-4401-98c1-fee04a7d2dd6\\_en?filename=2024%20](https://commission.europa.eu/document/download/84aa3726-82d7-4401-98c1-fee04a7d2dd6_en?filename=2024%20EU%20Justice%20Scoreboard.pdf)

#### Ioana Mazilescu

Deputy Head of Digital Transition & Judicial Training Unit, DG for Justice and Consumers, European Commission

#### Katerina Entcheva

Policy officer, Digital Transition & Judicial Training Unit, DG for Justice and Consumers, European Commission

<[EU%20Justice%20Scoreboard.pdf](https://commission.europa.eu/document/download/84aa3726-82d7-4401-98c1-fee04a7d2dd6_en?filename=2024%20EU%20Justice%20Scoreboard.pdf)> accessed 10 January 2025.

7 Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation, OJ L, 2023/2844, 27.12.2023.

8 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, 73.

# Reflections on Introducing Artificial Intelligence Tools in Support of Anti-Fraud

Georg Roebling and Bogdan Necula\*

Over the coming years, new tools based on large language models (LLMs) and other artificial intelligence-based software are set to play an increasing role in many modern administrations, including in the anti-fraud domain. One might even argue that the prevention, detection, and investigation of fraud and associated illegal activities, which today involve processing and analysing an ever-growing volume of data of different types, are uniquely suited to the strengths of such tools. The authors of this article share some reflections on two particular challenges that authorities, which seek to harvest the potential of artificial intelligence for anti-fraud purposes, have to come to terms with: first, how to leverage the strength of artificial intelligence tools by identifying suitable use cases for the specific anti-fraud domain? Second, how to navigate the emerging regulatory framework considering in particular that the European Union's Artificial Intelligence Act has entered into force on 1 August 2024?

## I. Introduction

With the occasion of OLAF's 25th anniversary, the year 2024 has given us the opportunity to look back on the evolution of the European Anti-Fraud Office (OLAF) over the last quarter of a century through the prism of the Office's digital transformation. The present article will complement that retrospective with a timid glimpse into the digital future.

Today, we can safely assume that new tools based on large language models and other artificial intelligence-based software are set to play an increasing role in many modern administrations in the future, including in the anti-fraud domain. One would even be tempted to say that the prevention, detection, and investigation of fraud and associated illegal activities, which today involve processing and analysing an ever-growing volume of data of different types, are uniquely suited to the strengths of such tools of artificial intelligence (AI). As we are prudently embarking on this journey ourselves, the purpose of this article is to share some of our own reflections and observations.

As promising as the potential of AI is without doubt for anti-fraud work, it is not always straightforward for public authorities to practically harvest this potential. There are many issues authorities need to come to terms with when it comes to practical implementation, three of which stand out. Addressing these issues decisively is likely to be key to the success of any such initiative.

First, public authorities need to identify for which anti-fraud-specific functionalities, or "use cases", in line with their own mandate they want to deploy an AI tool. To this effect, they need to conceptually link the strengths of AI tools to the specific requirements of making anti-fraud investi-

gations more efficient and more effective. In other words, investigators and technical staff have to be on the same page. Authorities then also have to match and adapt existing AI technology to map the resulting use cases, which is likely to require some additional technical enhancements (such as fine-tuning and prompt engineering). They would also have to ensure adequate protection of confidentiality of any data handled, as required by the use case at hand. Section II below offers some initial thoughts on these conceptual foundations for any anti-fraud engagement with AI.

Second, public authorities will of course need to be scrupulous in ensuring compliance with the legal framework. The use of AI tools, especially in a context as sensitive as anti-fraud prevention and investigation, raises important ethical issues, even if the AI tool will always be limited to a mere support role. An effective protection of the rights of citizens, including notably those enshrined in the Charter of Fundamental Rights of the European Union, is imperative. The legal framework has recently evolved with the adoption of the EU's AI Act. Having that act now in force since 1 August 2024 is an important step forward in terms of legal certainty when deploying AI. At the same time, some of the terms used in the AI Act are novel, and certain concepts are still to be fleshed out further by implementing and delegated acts and guidance. In addition, authorities wishing to deploy AI tools to support their anti-fraud work will need to be mindful of the applicable data protection regime – in the case of OLAF Regulation 2018/1725. Some of the regulatory cornerstones of the emerging legal framework for AI tools relevant for anti-fraud work are summarised in Section III below.

Third, public authorities must check the – internal or external – availability of the relevant technical skills to carry out



AI projects. This aspect may well influence the degree to which an anti-fraud authority engages with AI. We will not further explore the practical challenges linked to the availability of skills in this article. At this point, we would just like to mention the fact that OLAF, on behalf of the European Commission, annually awards grants to national authorities to build up their anti-fraud capacities to protect the Union's financial interests, in implementation of the Union Anti-Fraud Programme. Supporting Member States' digital capabilities is a stated priority, which would naturally include building up AI expertise.

## II. The Potential Use of AI Tools for Anti-Fraud Work

The dramatic leap forward in AI development in recent years has been transforming many industries, and its potential to revolutionize the anti-fraud domain is equally evident. AI developments could considerably facilitate certain steps in fraud prevention, detection, and investigation, particularly those that require an analysis of large volumes of data. Moreover, the power of AI tools cannot only make anti-fraud work more efficient, but also more effective. For example, AI tools may well pick up certain patterns in large data sets which can easily escape the human eye.

The following outlines some potential use cases of AI for anti-fraud preventive and investigative work from the perspective of natural language processing and image analysis. There will be a particular focus on how these technologies leverage large data sets to improve investigations.

### 1. Potential AI scenarios for anti-fraud work

One of the primary ways in which large language models (LLMs) can assist is through the analysis of text-based data. When pursuing anti-fraud investigations, investigators often deal with an enormous volume of text, including forensically acquired media, financial records, communication records, open sources data, and project-related documentation. As it stands, LLM technologies can contribute to automating the analysis of this data, extracting key information, identifying trends, and flagging suspicious communication. However, such analysis will have to be carefully reviewed by investigators in all cases for the reasons explained in section 2.b.

Considering an investigation's timeline, there are two main activities that define the world of anti-fraud: a) the prevention and pro-active detection of fraud and b) the reactive part, which is the actual investigation.

#### a) Use cases in the field of prevention

From a technical perspective, preventive tasks are dominated by risk analysis – a field in which advanced AI is already making good progress and is actively being tested by many software vendors. The risk analysis domain is technically quite complex due to the challenges surrounding data availability and the number of variables to be taken into account; hence, having AI assistance could generate additional insights.

**Risk analysis** on its own is already a conceptual challenge, simply when it comes to deciding on the scoring and the weights assigned to each risk and the calculations for the overall system. Here, the new AI technology can come into play by adding an understanding of qualitative risks. Furthermore, in light of the latest developments (especially the agentic approaches in which AI systems can carry out certain technical tasks autonomously, with minimal human intervention), a promising avenue would seem to be to test risk scoring systems in an automated manner with the help of **agentic systems**. This potential implementation presents the opportunity to run multiple risk approaches and, based on known true positives, to decide on the efficiency of the system.

Moreover, the field of prevention also includes verification of deliverables. In many cases, project deliverables are documents. Until now, the focus of these checks has been mostly on **plagiarism**, which is a complex issue. With the advent of generative AI, it has become easier for ill-intended individuals to alter text; as a consequence, traditional plagiarism checkers that focus on similarity will fail in flagging potentially copied texts. However, the same tools that serve the fraudster can be used to apply detection and indicate text similarity approximation.

#### b) Use cases in the field of investigation

From an investigative perspective, the use cases that benefit from advanced AI utilisation are already much clearer and well formulated.

For example, AI can be used to sift through numerous elements in forensically acquired media for **keywords or phrases indicative of fraudulent intent**. By processing large volumes of text, in combination with various helper techniques, LLMs can spot anomalies or unusual patterns of communication that may signal criminal intent. Additionally, AI-driven text analysis tools can be used to identify connections between seemingly unrelated elements. For instance, by analysing language and terminology used in certain email content, AI systems may discover **patterns in the modus operandi** of fraudsters.

Another potential application of AI in text analysis is **automated summarisation**. By using AI tools, investigators can generate summaries of large reports, saving valuable time in reading and analysing documents. For example, investigators are enabled to quickly review summaries of investigation reports, witness statements, or intelligence analysis reports, allowing them to focus on verification and decision-making – rather than the manual task of reading lengthy documents to extract relevant information. This can significantly enhance the speed of investigations and response times, especially when trying to gain an overview of the state of a case.

Object detection systems are also becoming increasingly sophisticated, allowing AI to **identify and track items**. As an example, customs is facing significant challenges in building efficient analytics for the quick aggregation of various data that appears in a normal customs workflow. It is standard for a customs investigation to deal with customs declarations, either in digital or scanned formats, images of containers and lorries, images of the contents of the containers, etc., on a regular basis. In many instances, this wealth of data must be aggregated and queried for an efficient investigation. By exploiting machine learning and optical character recognition, users can extract some information available in these images in some of the situations.

Another use case, also part of the challenges related to vision, is using **geo-located data**, such as aerial images of places of interest. AI models are becoming more and more efficient at identifying the typology of images and thus facilitating comparison between existing labelled data sets and the image of interest. One of the most relevant benefits is that AI-based object/area recognition greatly reduces the human effort and potentially the number of false positives for manual review.

**Financial transaction analysis** is another domain that AI may impact in a significant manner. Data sets of hundreds of thousands of lines of transactions appear to be the ideal environment for AI, with the purpose of identifying fraudulent behaviour. In everyday work, an analyst would have numerous tools and methods available to sift through these data sets and try to pinpoint financial flows, anomalous transactions, matching amounts, relevant details within a transaction description, etc. Thus, LLMs might not be the first tool designed to handle financial transactions. However, initial results in this field indicate that AI capabilities could be of great benefit, especially when dealing with the transaction description from a natural language understanding perspective.

Last but not least, the **pre-processing and visualisation of data** is one of the biggest daily challenges of many opera-

tional intelligence analysts. LLMs can significantly enhance tasks such as entity recognition, entity resolution, co-reference resolution, and building network graphs, which are critical in complex data analysis for fraud investigations. **Entity recognition** involves identifying key entities like people, organisations, and locations within unstructured text. **Entity resolution** is the process of determining whether different mentions refer to the same real-world entity, which is especially useful in fraud investigations where names or identifiers may vary across data. The term **co-reference resolution** involves linking different mentions of the same entity within a text (e.g., resolving “he” or “the company” to the correct entity), allowing for a more coherent understanding and tracking of entities across documents. Once entities and their relationships have been identified, LLMs can assist in constructing network graphs that visually represent the connections between entities. These graphs enable investigators to uncover hidden relationships, visualise fraud patterns, and detect suspicious networks more effectively.

## 2. Challenges, limitations, and potential solutions

The previous section only sketched out some of the possible ways in which AI tools are likely to support anti-fraud prevention and investigations in the near future. Many more use cases will almost certainly appear over the coming months and years. Yet as tempting as the power of these AI tools will be for many anti-fraud authorities struggling with scarce resources, employing this technology also has limitations, such as notably the imperative to systematically and critically review the AI output by humans. This section explores some key challenges and limitations whilst at the same time attempting to point to potential solutions.

a) One of the most critical aspects of using AI in investigations, especially when working with LLMs for tasks like text analysis, is **prompt engineering**. This term refers to the process of designing specific inputs or prompts that guide AI models, particularly LLMs, to produce desired outputs. In practice, the concept of prompt engineering involves understanding how to effectively communicate with AI models to generate accurate, relevant, and context-specific outputs. To develop skills in prompt engineering, agencies may focus on understanding the AI model’s capabilities and limitations – i.e., how it works, what data it was trained on, etc. – iterative testing and comparing the results, and researching prompt libraries and tools.

To enable successful prompt engineering in the context of an investigation, it is also important that the AI tool is familiar with **domain-specific language**. For example, as mentioned, AI might be used to summarise various documents, such as

intelligence analysis reports. However, the quality and relevance of the output depend heavily on how the input data is framed. If the prompts are not carefully constructed, the AI system might produce misleading or irrelevant results.

One of the key challenges of prompt engineering is ensuring that LLMs can understand and process the nuances of specific language. Data often contains jargon, abbreviations, or domain-specific terms (e.g. procurement), that may not be easily interpretable by AI models without specific contextual guidance. Moreover, both commercially available and open source LLMs are trained on general data sets and might not fully comprehend the domain-specific knowledge required for anti-fraud investigations.

To overcome this, prompt engineering requires deep collaboration between AI developers and professionals in the field. For instance, a well-engineered prompt might ask the AI tool to summarise reports by focusing on specific details like fact descriptions, modus operandi, or location. If designed correctly, prompt engineering can guide LLMs to provide accurate and contextually relevant insights.

b) Another major issue with LLMs, especially when applied to specialised fields like investigations, is the phenomenon of “**hallucinations**”. This term refers to instances where AI models generate plausible-sounding but inaccurate or entirely fabricated information. For an investigation, relying on inaccurate data could have serious consequences. Hallucinations in LLMs arise because these models are often trained on broad data sets that do not always include the specific, factual information required for legal or investigative tasks. As a result, when asked to generate text based on prompts, the model might “fill in the gaps” with information that sounds reasonable but is not grounded in reality. As a consequence, we need to be cautious when using LLMs, ensuring that AI outputs are always verified by human experts to avoid the risks associated with incorrect information.

c) One emerging technique that helps mitigate some of the limitations of LLMs is **retrieval-augmented generation (RAG)**. RAG is a hybrid approach that combines the generative capabilities of LLMs with retrieval-based methods. In this system, instead of relying solely on the AI’s pre-trained knowledge, the model first retrieves relevant information from a structured database or external knowledge source before generating a response.

This approach is particularly useful for anti-fraud tasks, where accurate and up-to-date information is crucial. For instance, instead of relying on the LLM to generate an answer from general knowledge, RAG-enabled systems are able to

first retrieve relevant data from internal databases. AI then uses this specific information to generate a more accurate and contextually informed output. This minimises the risk of hallucinations and enhances the reliability of AI-generated insights.

d) **Reinforcement Learning from Human Feedback (RLHF)** is another emerging approach that combines traditional reinforcement learning with direct human input to improve the behaviour and performance of AI systems. This technique allows AI models, particularly LLMs, to learn more effectively from human preferences, judgments, and corrections, leading to more aligned, accurate, and user-friendly outputs. RLHF is especially valuable in areas where human interpretation, ethics, or nuanced decision-making play a critical role, making it a key tool in refining AI systems for real-world applications.

At its core, reinforcement learning (RL) involves training an AI agent by rewarding desired behaviours and penalising undesirable ones. In RLHF, humans play an active role by providing feedback in the form of rewards or corrections to guide the AI model’s learning process. Instead of relying solely on predefined rewards from a static environment, RLHF allows humans to directly assess the outputs of AI and intervene when AI produces incorrect, unethical, or sub-optimal results. This human feedback becomes a part of the reward mechanism, refining AI in its actions and decisions over time.

RLHF addresses several challenges that traditional AI training methods face, particularly in areas where objective measures of success are difficult to define. For example, in language models, it can be hard to quantify what constitutes a “good” response, as quality often depends on context, tone, and user intent. Human feedback provides the nuance that purely automated systems might lack. In practical terms, human annotators may review AI outputs and rank them based on quality or relevance, enabling AI to adjust its future responses based on this feedback. This iterative process continues until the AI system becomes more aligned with human expectations.

e) Although not strictly connected to advanced AI, the **security of data** manipulated in an AI framework should continue to be a top concern for practitioners. Many of the existing tools employ API (Application Programming Interfaces) and services in clouds to serve AI-generated content to users. In general, the terms of use can bring some piece of mind to concerned users. However, the general recommendation whenever such tools are used for investigative purposes is to build systems in protected environments, ideally

segregated from the internet and with models and software that can be installed locally without additional resources.

f) Apart from the technical aspects, anti-fraud authorities planning to engage with AI may also wish to, from the outset, reflect on how to deal with **staff attitudes** towards this new technology. An informal (and not necessarily representative) survey at a recent conference with anti-fraud practitioners from the Member States and the Candidate Countries showed that the attitudes of those present fell into two groups of comparable size: Whilst respondents in one group highlighted the potential and benefit of AI for anti-fraud work, another group had reservations about such AI use, notably on account of privacy and ethical concerns. Some respondents were also wondering how AI would affect their current job.

Authorities may thus consider developing a training strategy to upskill staff as well as a parallel one on communication and awareness raising to pro-actively engage with staff on their legitimate questions and concerns. And of course, since key components of the emerging regulatory AI framework are precisely designed to address some of those questions, attention to full regulatory compliance may be a part of the answer.

### III. Key Elements of the Emerging Regulatory Framework

This section explores some of the basic regulatory parameters which govern the use of AI by public authorities in the anti-fraud domain today. Adhering to these parameters is a precondition of deploying AI tools in full compliance. But in addition, their existence may also in itself influence which AI use cases an authority may wish to pursue based on a cost-benefit analysis.

As explained in the AI Act, the use of AI systems by law enforcement raises particular concerns. This is notably due to what the Union legislator perceives as a power imbalance, and on account of the grave consequences that law enforcement action can have, such as surveillance, arrest, or the deprivation of a natural person's liberty. In law enforcement, any possible discriminatory or in other ways unethical bias on the part of an AI tool could lead to unacceptable outcomes. Moreover, the use of an AI tool – with its autonomously generated, not totally predictable outcomes – is inevitably somewhat at odds with a law enforcement context where, according to Recital 59 of the AI Act, “accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress.”

#### 1. The AI Act

To address these concerns, the AI Act introduces certain substantive and procedural guardrails. It is designed to improve the functioning of the internal market by laying down a uniform legal framework for the development, the placing on the market, the putting into service, and the use of AI systems in the EU in accordance with its values, and to promote the uptake of human-centric and trustworthy AI whilst ensuring a high level of protection of health, safety, and fundamental rights.

To achieve these objectives, the regulatory approach taken in the AI Act is reminiscent of the risk-based regulatory layers familiar from product safety rules (the pyramid-shaped “hierarchy of hazard controls”) that apply to some categories of goods placed onto the internal market. In this spirit, the AI Act in essence distinguishes between the following:

- The most harmful AI practices, which will be prohibited (Art. 5);
- High-risk AI systems to which rather stringent regulatory requirements apply (Art. 6(2) in combination with Annex III); and
- Less risky AI systems which remain largely unregulated.

#### a) Application of the AI Act for anti-fraud projects

The first question that needs to be clarified is of course whether an envisaged AI project that would support fraud prevention or investigation would actually fall into the scope of the AI Act.

(aa) *De ratione temporis*, the AI Act has been in force since 1 August 2024. However, its main provisions will only be **phased in progressively**: the prohibitions set out in Art. 5 will apply as of 2 February 2025, and the rules on high-risk AI systems referred to in Art. 6(2) in combination with Annex III only apply as of 2 August 2026. High-risk AI systems already on the market prior to that date will in principle only have to comply with the AI Act if they are subject to significant changes in their designs. However, public authorities that are deploying AI tools that were on the market before the cut-off date will nevertheless have to comply with the AI Act by 2 August 2030 at the latest.

(bb) Today, many anti-fraud authorities already deploy a variety of analytical tools that operate on the basis of advanced algorithms, for example for fraud detection. This can sometimes give rise to doubts as to whether those systems would – possibly retroactively – fall under the AI Act. It is therefore important to delineate its scope of application *de ratione materiae* as well. Art. 3(1) of the AI Act contains the



relevant definition in that regard: The Act applies, as a matter of principle, only to **machine-based systems which infer**, from the input they receive, how to generate output such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. The meaning of the decisive key term “infer”, which arguably suggests some degree of *autonomous* output generation, will without a doubt be further elaborated in the future.

(cc) It should also be noted that **any research, testing, and development** activity regarding AI systems before these are put into service do not fall into the scope of the AI Act, as long as no testing under real-world conditions is undertaken (e.g., experimenting with live data from a database). Special rules, including a pre-authorisation or registration process, apply where the testing of high-risk AI systems is carried out under real-world conditions. The subjects of such testing should also give their informed consent prior to the tests.

### b) Prohibition of a project?

If an AI tool to be developed were to, as a matter of principle, lie within the scope of the AI Act, it is of course imperative to ascertain early on whether such a tool would fall into the **prohibited categories** set out in Art. 5 of the AI Act (see above). For the present purposes, the prohibited practice which arguably comes closest to typical anti-fraud work concerns an AI-based assessment of the risk of natural persons committing a criminal offence. However, that clause only applies if two conditions are fulfilled: (i) where the assessment is based solely on the profiling of a natural person, and (ii) where the AI system is not only used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity.

*Prima facie*, many of the risk analysis systems operated by anti-fraud authorities to detect expenditure or revenue fraud would not typically meet these conditions. In particular, in many cases those systems do not focus on natural persons, but on undertakings. In addition, it is difficult to imagine that these systems would be based exclusively on the profiling of a natural person. Moreover, they usually link their evaluation to objective and verifiable (but not necessarily verified) facts, such as previous infringements, or suspicious shipping routes. What is more, the assessment of whether a person is ultimately involved in a criminal activity will always be reserved for a human being, and never be automated – therefore the second of the two conditions above would not be met. Last but not least, Recital 42 of the AI Act adds further clarity in that regard: According to this section, the prohibition does not apply to AI systems using

(i) risk analytics to assess the likelihood of financial fraud by undertakings on the basis of suspicious transactions, or (ii) risk analysis tools to predict the likelihood of the location of narcotics or illicit goods by customs authorities, for example on the basis of known trafficking routes. Against this background, the prohibitions of the AI Act should not typically apply to the well-established risk analysis systems operated by many agencies (if ever those systems were to be classified as AI tools based on their advanced features; see above).

### c) High-risk project?

The regulatory requirements applicable to AI tools for anti-fraud purposes will then depend on whether a **high-risk** classification pursuant to Art. 6(2) of the AI Act is warranted. This provision refers to several specific categories of AI use cases set out in Annex III, which the Union legislator, in principle, deemed to present a higher risk. For the present purposes, Point 6 in Annex III dealing with the law enforcement area is the most relevant.

aa) Point 6 Annex III refers to certain activities by **law enforcement** authorities.

(1) The AI Act defines these authorities, as far as this article goes, as any public authority competent for the prevention, investigation, detection, or prosecution of a criminal offence or the execution of criminal penalties. It is reasonable to assume that this **definition** focusing on criminal offences does not cover mere administrative authorities. This view is, in our opinion, supported by Recital 59, which clarifies that AI systems specifically intended to be used for “the administrative proceedings by tax and customs authorities” are not to be classified as high-risk AI systems. It should also be noted that Point 6 is not limited to law enforcement authorities, but equally addresses AI systems intended to be used by Union institutions, bodies, offices, and agencies supporting law enforcement authorities.

(2) Point 6 of Annex III AI Act goes on to categorise a number of AI systems with specific functionalities as high risk. These notably concern AI systems

- “to evaluate the **reliability of evidence** in the course of the investigation or prosecution of criminal offences” (Point 6c);
- “for assessing the **risk of a natural person offending or re-offending** not solely on the basis of the profiling of persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups” (Point 6d); or

- “for the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of the detection, investigation or prosecution of criminal offences” (Point 6e).

As it is still early days, it is difficult to predict to what extent these categories will be practically relevant for the AI use cases which anti-fraud authorities may be considering at some point in the future. Suffice it to say that, first of all, from today’s perspective it is not easy to envision an AI system evaluating the reliability of evidence, but of course technologies are developing fast. Secondly, it needs to be underlined that the other two categories are limited to the profiling of natural persons for which the unlikelihood of relevance for anti-fraud AI tools has been already mentioned above under point 1b).

bb) However, even where an anti-fraud AI project to be evaluated could *prima facie* fall into one of the afore-mentioned three categories under point 6 of Annex III, the AI Act adds an important derogation of practical relevance: Pursuant to Art. 6(3), AI systems which perform certain types of **ancillary tasks** are not to be considered high risk. This relates in particular to AI systems intended to (i) perform a narrow procedural task, (ii) improve the result of a previously completed human activity, or (iii) perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III. However, before putting an AI system which the provider has concluded to not be high risk due to its ancillary nature into service, law enforcement authorities need to register it in a secured EU database.

cc) Classifying an AI system as high risk would have important further regulatory consequences. **Regulatory requirements** for high-risk AI systems are set out, notably, in Arts. 8 to 27 AI Act. They include, for example, the need to establish a risk management system (Art. 8), to draw up technical documents (Art. 11), and to keep records (Art. 12). In addition, transparency obligations (Art. 13) and obligations for facilitating human oversight (Art. 14) need to be fulfilled. Under certain conditions, a fundamental rights impact assessment will also need to be carried out (Art. 27). Many public authorities are set to carefully examine the expected costs and benefits which deploying a high-risk AI system would entail. However, it is beyond the scope of this article to provide details of these requirements.

## 2. Data protection rules

Next to the necessary compliance with the AI Act, the use of AI tools for anti-fraud purposes must also adhere to the **applicable data protection regime**. In the case of OLAF, this would be Regulation 2018/1725, applicable to EU institu-

tions, bodies, offices, and institutions. It is aligned to similar provisions in the General Data Protection Regulation (GDPR).

### a) Application of the data protection regime and overlap with the AI Act

The data protection rules naturally only apply to the extent that personal data is actually processed by an AI tool. This means that where an AI tool is deployed using data sets not containing such personal data (for example, container numbers, or vessel movements, as long as those elements cannot be linked to a specific person), the processing is out of **scope** of the applicable data protection regulation.

On occasion there may be some **functional overlap** between the requirements of the applicable data protection rules and the AI Act. For example, where a data protection impact assessment needs to be carried out, that analysis may in part address similar issues as those required as part of the Fundamental Rights Impact Assessment under the AI Act (see above 1 cc)). Likewise, the need for a data protection impact assessment depends on whether the processing of personal data as part of AI use is likely to result in high risks to the rights and freedoms of natural persons, taking into account the nature, scope, context, and purposes of the processing. The EU institutions would base their assessment on the Guidance and template for threshold assessment provided by the European Data Protection Supervisor. It remains to be seen whether, in making that assessment, they might take into account the Union legislator’s choice to exempt some ancillary AI from being considered high risk, pursuant to Art. 6(3) of the AI Act (see above 1 bb)).

### b) Implementation of key data protection principles

Given that this article can only outline the potential use of AI tools and the connected challenges in the anti-fraud area, and given the complex matter, this article cannot exhaustively discuss the application of the EU data protection regime to AI use by anti-fraud authorities. Hence, we wish to limit ourselves to highlighting certain **key principles** underpinning the applicable data protection regime, which should also be implemented when using AI for the kind of anti-fraud purposes described above.

First of all, when developing and deploying AI tools, it is essential to ensure that the processing of personal data is lawful, fair, and transparent. **Lawful processing** requires that the anti-fraud authority has a valid legal basis for the processing of personal data, and that the personal data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those pur-

poses. The processing must also be necessary for the performance of the task of the anti-fraud authority. In addition, the authorities must implement appropriate technical and organisational measures to ensure the security and confidentiality of the data, including the use of encryption and access controls.

Anti-fraud authorities must be **transparent** about the use of AI tools in the processing of personal data. This includes providing clear information to individuals about the use of AI tools, the types of data being processed, and the purposes of the processing. Individuals must also be informed about their rights, including the right to access, rectify, and erase their personal data.

Anti-fraud authorities using AI for purposes that involve personal data need to be mindful of the **data minimisation** principle. When looking at the illustrative AI use cases presented in Section II above, limiting the exposure of personal data to the AI tool to only a small sub-set of data (e.g., one case file only), rather than a whole database, could be one of the possible means of implementing the data minimisation principle. Such a limitation, however, must be compatible with the intended use case.

Anti-fraud authorities will naturally also be very mindful of the fact that in the context of AI use, personal data is processed in a manner that ensures appropriate **security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. In particular, it can reasonably be expected that anti-fraud authorities would not normally work with internet-based AI tools created by third parties when confidential information, including personal data, is involved; instead, they would operate their AI tool in a more secure IT environment. In addition, the usual access control limitations familiar from the general IT system will often need to be applied.

Moreover, AI tools must not become a way to undermine **data access policies** based on a need-to-know principle by allowing the accidental or intentional disclosure via an AI output of data to which a user would not normally have access.

Since compliance with data protection rules is of fundamental importance to anti-fraud authorities planning to use AI on data sets containing personal data, they are well-advised to integrate this dimension into the design of their AI system right from the start (**data protection by design**). The data minimisation and confidentiality principles mentioned previously are possible elements in such a design approach. Another possibility may be to focus on the design of the input

interface. Where users of an AI tool can engineer prompts as they wish, there is always the hypothetical possibility that a rogue user might abuse the power of the AI tool for purposes not compatible with the mission of the public authority. Such abuse can be largely eliminated with a different design, in which the system administrator configures the user interface in such a way that only pre-defined prompts are available to regular users.

#### IV. Conclusions

The field of AI is developing at a fast, not to say furious, pace. New models with substantially expanded capabilities are being released by the major providers several times a year. Keeping up with these developments is a challenge to all actors, so there will inevitably always be some element of learning by doing.

Anti-fraud authorities are working with limited resources whilst the data volumes they have to deal with are growing exponentially. The processing power of especially the latest generative AI tools give hope that they can help authorities to stay on top of the game. To harvest this potential, authorities will, however, have to invest in the technical and intellectual infrastructure, i.e. to build up the relevant technical and user expertise. OLAF has begun supporting national authorities on this challenging but promising trajectory as concerns the protection of the Union budget.

At the same time, anti-fraud authorities need to be mindful of the limitations and constraints of AI tools. This applies both from the perspective of the inherent technological limitations of such tools (such as potential bias and hallucinations), and from a privacy perspective. For these reasons, it is clear that AI tools will always be limited to a support role in anti-fraud prevention and investigation. The objective of the prudent use of AI by anti-fraud authorities must be to render the decision-making of human anti-fraud investigators more efficient and effective, and never to replace it.

---

\* This article only reflects the authors' personal opinions and cannot be attributed to the Institution that employs them.

1 See eucrim issue 4/2024 (forthcoming).

2 See also, from a general law enforcement perspective, the discussion of these matters in Europol, *AI and policing – The benefits and challenges of artificial intelligence for law enforcement*, 2024, available at: <<https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf>> accessed 9 December 2024.

3 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on arti-

**Georg Roebling**

Head of Unit “Intelligence & Operational Analysis”,  
European Anti-Fraud Office (OLAF)

**Bogdan Necula**

Deputy Head of Unit “Intelligence & Operational  
Analysis”, European Anti-Fraud Office (OLAF)

ficial intelligence and amending certain Regulations and Directives (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

4 See D. Hadwick, “‘Error 404 – Match not found’ – Tax Enforcement and Law Enforcement in the EU Artificial Intelligence Act”, (2023) *eu crim* 55–60.

5 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, 39.

6 See for example the 2024 Call for proposals for the Union Anti-Fraud Programme (EUAF), available at: <[https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/euaf/wp-call/2024/call-fiche\\_euaf-2024-ta\\_euaf-2024-trai\\_en.pdf](https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/euaf/wp-call/2024/call-fiche_euaf-2024-ta_euaf-2024-trai_en.pdf)> accessed 9 December 2024.

7 The financial transaction typically has a description field that, from

a data perspective, is a free text field. It usually contains details of the transactions, in many cases with valuable insights such as invoice number, contract reference, explanation for the payment, etc.

8 See Recital 59 AI Act. For the concerns, see also D. Kafteranis, A. Sachoulidou, and U. Turksen, “Artificial Intelligence in Law Enforcement Settings – AI Solutions for Disrupting Illicit Money Flows”, (2023) *eu crim*, 60–66, in particular Chapter IV.

9 See Recital 1 AI Act.

10 Art. 113(a) AI Act.

11 Art. 113 AI Act.

12 Art. 111(2) AI Act.

13 Art. 111(2) AI Act, last sentence.

14 Art. 2(8) AI Act.

15 See Art. 60(4) AI Act.

16 Art. 61(1) AI Act.

17 Art. 5(1)(d) AI Act.

18 See the legal definition in Art. 3(45) AI Act.

19 See Art. 49(4) AI Act.

20 Art. 2(7) AI Act.

21 *Op. cit.* (n. 5).

22 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 199, 4.5.2016, 1.

23 See for example ECJ, 9 November 2023, Case C-319/22, *Autoteile-Handel*, para. 45 with reference to the earlier judgment of 19 October 2014, Case C-582/14, *Breyer*, paras. 43 et seq.

24 See Art. 2(1) Regulation 2018/1725.

25 See Art. 39 Regulation 2018/1725.

26 See European Data Protection Supervisor, “Data Protection Impact Assessment (DPIA)” <[https://www.edps.europa.eu/data-protection-impact-assessment-dpia\\_en](https://www.edps.europa.eu/data-protection-impact-assessment-dpia_en)> accessed 9 December 2024.

27 Art. 4(1)(a) Regulation 2018/1725.

28 Art. 5(1)(a) Regulation 2018/1725.

29 Art. 4(1)(c) Regulation 2018/1725.

30 Art. 4(1)(d) Regulation 2018/1725.

31 Art. 27(1) Regulation 2018/1725.

# Data-Driven Investigations in a Cross-Border Setting

## Experiences from the Netherlands

Boudewijn de Jonge and Barry de Vries\*

Current technology enables drug traffickers and other criminals to live like digital nomads and direct global operations from any location in the world. That said, this surge of technology also provides law enforcement with new tools. Large datasets allow us to change the way we conduct investigations, making a data-driven law enforcement approach possible. No data-driven investigation can ignore the international dimension of organised crime. In this article, the authors analyse some of the challenges and achievements they see in cross-border data-driven investigations, in the light of the standards of the Law Enforcement Directive.



## I. Introduction

Many have been suggesting that we are currently witnessing the advent of a totally new technological era. Our societies are changing due to the democratisation of technology and the incredible power of those technologies. In the individual Member States of the EU, many initiatives have been launched by law enforcement and the judicial sector to explore how technology can be exploited for fighting crime and administering justice. The police force of the Netherlands is no exception and strives to be amongst the most innovative forces in Europe, with data-driven policing being one of the four pillars of their multi-annual strategy.<sup>1</sup> In this article, we share some of our experiences with data-driven work in cross-border cases.

In section II, we explain and illustrate the data-driven investigation strategy that is being followed in the Netherlands. In section III, we look at some of the lessons learned in the Netherlands and relate those to European law, including the Law Enforcement Directive (LED).<sup>2</sup> The perspective of cross-border cooperation is the topic of section IV, from which we draw some conclusions for future practice in section V.

## II. Data-Driven Investigations

In line with technology having become more widespread and powerful, criminal investigations have gained access to ever larger data sets. In the fight against child pornography, for example, the exchange and cross-border matching of large data sets has long been a cornerstone of investigative work.<sup>3</sup> Likewise, the seizure of darkweb servers, including servers of illegal marketplaces, has created dazzling amounts of data; in some instances, investigating one such seizure has resulted in as many as hundreds of criminal cases. Yet, the hacking of the encrypted communication services EncroChat and SkyECC has represented a turning point when it comes to assessing the necessity of and control over the use of such data sets. Along with the availability of large data sets, new ways of policing have been invented.

Data-driven work in the investigative police branch is now considered a crucial component of the strategy of the Dutch police. Data-driven methodologies provide new opportunities for tackling criminal activities more efficiently and effectively. This goes beyond the mere obtaining and analysing of a large data set.

This strategy is rooted in the notion of problem-oriented policing shaped by *Herman Goldstein* in the 1990s.<sup>4</sup> Build-

ing on that theory, the concept of intelligence-led policing was developed at the beginning of the 21st century. Another crucial step was to incorporate social network analysis into policing, one proponent being *Paul Duijn*.<sup>5</sup> This systematic approach and use of data has the potential to identify key actors and relationships, disrupt critical connections, unveil hidden structures, prioritize vulnerabilities and minimize collateral damage.<sup>6</sup> By using this systematic approach, police can focus their efforts on key elements within a network rather than applying broad or generalized approaches. Combining the problem-oriented approach with network analysis and adding large data sets and technology offers a comprehensive framework for modern policing. We now have the tools to analyse data sets, identify patterns, trends, and connections within criminal networks more quickly and accurately. Next to enabling more targeted interventions, this integration allows police to dismantle organisations as such and develop proactive strategies. The outlined strategy differs fundamentally from starting an investigation based on a single incident, such as the seizure of one drugs transport or intelligence about a single criminal organisation.

This can be illustrated by the SkyECC case, in which police revealed that messages from dozens of cocaine traffickers had been exchanged via the encrypted communication service SkyECC; the data obtained by hacking the service served as evidence of an industry that functions as an interconnected global network, supported by various enablers.<sup>7</sup> The authors witnessed the clever use of logistics chains, complex financial schemes, and the use of encrypted apps.<sup>8</sup> The higher echelons of drug trafficking organisations live like digital nomads and organise complex supply chains residing, for example, on the Mediterranean coast. The distribution of these drugs from a Western European port to the end users takes only days, sometimes hours.<sup>9</sup> In this fast-moving market, it is difficult for national law enforcement to make a lasting impact. A data-driven approach represents one attempt of formulating a response to that complex criminal industry.

As organised crime benefits from operating across borders and has characteristics of a global industry, a data-driven police approach must also address the challenges of cross-jurisdictional collaboration. Criminal organisations often exploit international boundaries to evade law enforcement, requiring a coordinated effort between local, national, and international agencies. By combining problem-oriented strategies with network analysis and leveraging big data, police forces can better anticipate and respond to transnational crime, targeting the key nodes and connections that sustain global criminal networks.

### III. Some Lessons from the Netherlands

A data-driven approach to criminal investigations should result in admissible and understandable evidence in court. In a learning-by-doing process, three standards have been carved out to ensure reliable output that can be used in court: (1) clean data; (2) transparency, and (3) collaborative design. Whilst these standards primarily serve the admissibility and evidential value of the data in court, we will show how they align with the privacy standards of the LED.

#### 1. Clean data

Clean data, which is accurate, consistent, and free from errors or duplicates, is crucial for drawing reliable conclusions and making informed decisions. Minor inaccuracies or biased selection of data can lead to significant misinterpretations. Therefore, ensuring data integrity and cleanliness is essential for law enforcement to effectively understand and act upon the insights derived from big data.

For example, it can occur that the timestamp of a message is inaccurate or a message is replicated for technical reasons. In order to easily read and correctly interpret the evidence, technical errors may be corrected in the data set. Yet, at all stages of processing this initial correction will have to be visible and traceable. Secondly, the reason for the correction is to be explained. By doing so, all parties to the trial and the court will be able to properly evaluate the evidence and the correction, and compare it to the original uncorrected data if requested.

Data-driven investigations are able to bring together data sets of different origins and quality. For example, travel data combined with encrypted communication might reveal logistical hotspots of criminal goods. Or the book-keeping of a criminal facilitator combined with an analysis of FIU information might reveal illicit money flows of his clients. Moreover, a large data set gathered in one case may later become relevant for another investigation. The combination of such datasets offers new insights.

In order to maintain data quality and ensure consistency, the Dutch police follows the CSAE model when handling large data sets. “CSAE” is a cycle and stands for the four phases of the process: Collect, Store, Analyse, and Engage.<sup>10</sup>

The *Collect* stage focuses on gathering data from various sources, such as crime scenes, former investigations, digital devices, and large data sets (e.g., encrypted communication). Next, the *Store* stage ensures that all collected

information is securely stored in information management systems preserving it for further analysis. In the *Analyse* stage, forensic tools and techniques are used to examine the evidence, identifying patterns and connections between suspects, victims, and crime scenes. Lastly, in the *Engage* stage, interventions take shape. Interventions may range from searches and arrests within the framework of a criminal investigation, to enabling administrative authorities to act within their respective competences.

The output can be used as evidence in a criminal investigation or to disrupt criminal activities, for instance by taking a criminal marketplace offline. In particular with cross-border crime, criminal prosecution of foreign-based networks may be impossible and disruption of the crime may be a more realistic option.<sup>11</sup> The results of the interventions will be fed back into the loop in the form of new data, closing the cycle.<sup>12</sup>

So what role does the LED play in this context? Amongst others, it requires that the data processed are adequate, relevant, and accurate.<sup>13</sup> Whereas the significance of these principles seem indisputable, one may wonder how exactly they play out with large data sets. Initial, unedited data will include (technical) errors, mistakes, and inaccuracies. Yet the authentic, unedited copy is of tremendous importance for later verification of evidence by the parties to the trial. As to data minimization, storing only the “relevant” parts of a data set brings about the risk of eliminating exculpatory evidence. Another problem with that principle arises in connection with the identification of (criminal) users of an anonymous communication network. It is hard to predict whether and when a positive identification can be made.

In the Netherlands, for example, the first large data set obtained by the police resulted from the decryption of communications on the Ennetcom network in 2016. It consisted of a few million messages obtained when a server was seized in Canada. Initially, only a small number of users could be identified. However, the data came back into focus when other providers of anonymous communication services were hacked, providing new leads for the identification of users of the Ennetcom service. Several murder cases involving Ennetcom users did only end in court very recently.<sup>14</sup> It was thus only after many years that accuracy and relevance of the data became clear, and the wider data set became of relevance to the defence to search for exculpatory evidence. This example calls for caution against a too strict interpretation of the principles of Art. 4 of the LED. An original, unedited copy of the data may have to be kept for a very long time.

## 2. Transparency

Data-driven investigations ultimately serve justice. An accusation will have to be sustained in the courtroom, and the quality, reliability, and legality of the evidence presented may be tested there. Transparency on the basis of the collection of data, and logging of procedural decisions is thus crucial to sustain the subsequent penal or administrative actions. Accountability must be ensured during all steps of a data-driven investigation; this is essential for upholding legitimacy.

Yet the challenge is that hundreds or even thousands of court cases may follow from the collection of a single data set. Art. 4(2) of the LED permits the collected metadata of one criminal group to be further processed in new investigations.<sup>15</sup> Take the example of the metadata of one single, powerful organised crime group being intercepted while its members were communicating over the SkyECC platform. This metadata revealed insights not only into the group's own dealings, but also into their contacts with other criminals outside the group. When analysed further, this led to new groups being identified. In this new case, the defence was provided with the original interception warrant, but the court did not find it relevant for the defence to know which other contacts were identified.<sup>16</sup>

In other cases, it has been debated whether the defence ought to be given access to complete data sets, given that receiving only a copy of the data pertaining to the accused person alone might feel too restrictive.<sup>17</sup> In some cases, Dutch courts have allowed the defence to read other persons' communications, or provided a list of keywords to search the entire data set.

Restricted access to the original data for the defence has not been the only point of contention; it has been argued that the same tools should be made available as were available to law enforcement.<sup>18</sup> In the Netherlands, discovery by the defence is now facilitated by the very same tool that the police uses, tailored to the selection of data relevant to the case at hand. The platform *Hansken*, developed by the national forensic institute, enables the consultation of large data sets.<sup>19</sup> The defence may now be granted access to this data, both on site and remotely.

## 3. Collaborative design

The standard of transparency requires planning ahead, thinking of the ultimate test in court. It is key to involve all actors from an early stage, in this instance the prosecution service. In the EncroChat and SkyECC investigations, there

was an intense collaboration between the police and public prosecution service to ensure the data could be used in court. This did not only help to ensure that innovation was developed in line with the classical rules of criminal procedure, it also ensured focus in the phase of analysis.

A data-driven law enforcement approach offers a new way of improving the efficiency of criminal justice<sup>20</sup> and of bringing about more impactful judicial interventions. Law enforcement analysis on SKYECC revealed, for instance, an essential element to the thousands of drug transactions: an underground banking system.<sup>21</sup> By searching the data – in conformity with the judicial warrants –, various global underground bankers were identified that had been processing transactions worth hundreds of millions of euros each.<sup>22</sup> In consequence, that analysis has inspired the public prosecution to dedicate more attention to the phenomenon of underground banking.

Another advantage of the involvement of the prosecution service in the early stages of data-driven investigations is that cases can be more properly selected. A criminal investigation traditionally starts from a position of suspicion, followed by a search for evidence, either incriminating or exculpatory. Conversely, today's abundance of data evidence allows us to select markets, subjects and regions. It allows us to decide to prosecute a single key player in an individual case, or to prosecute an entire network in a large-scale trial. These choices in the investigation have far-reaching effects on the way a trial is organised and – indeed – the capacity needed further down the chain. As this concerns prosecutorial strategies, these choices are usually made jointly by the prosecution and the police.

The study of the first deciphered messages from EncroChat brought about an important insight, which proved relevant for any work with the data in general. In most cases, it appeared very difficult to prove which one of numerous conversations on drug transactions did actually result in a deal or international drug transport. Yet, each conversation constituted an inchoate crime, i.e. that of making preparations for drug trafficking. This allowed the police to change their selection of cases, given the limited capacity of the police, prosecution service, and the criminal courts: the best way forward was to reason backwards. There was sufficient proof against the average EncroChat user for dozens of separate inchoate crimes. Yet, in most cases they were only accused of a limited number thereof; usually the more serious ones. The goal was to optimize the use of resources in order to achieve the best result. In this way, resources of the police could be conserved, case files limited in size, and trials shortened.

Clearly, these choices have only been possible because the Dutch criminal justice system allows for a wide prosecutorial discretion. However, another important element in this selection and prioritization process is the collaborative effort in the early phases of analysis. Proper guidance and insight into the capacity of the partners prevented the system from collapse.<sup>23</sup>

#### IV. International Cooperation in Data-Driven Investigations

Organised crime often takes place in a transnational setting. This international context poses additional challenges for a data-driven law enforcement approach when fighting organised crime. The following outlines these challenges.

##### 1. Burden sharing and solidarity

It is general consensus that there is a necessity to respond to digitalised crime. However, in the context of large data sets, jurisdictional problems for police and judicial authorities arise. It is often unclear at the beginning of an investigation where exactly the users of a platform or service are based, and where most of the crimes have been committed. In some cases of transnational organised crime, international public law stipulates an obligation to investigate and cooperate on cross-border crime, such as Art. 11(2) of the Palermo Convention.<sup>24</sup> There are only a few pan-European agreements that include a fair distribution of cases.<sup>25</sup> Yet, in many more cases, it will depend on the personal motivation and solidarity of the involved law enforcement and judicial actors to work on cases that may initially have a very limited link to their own jurisdiction.

A praiseworthy example in this context is how certain German police and prosecution services have taken action against darkweb marketplaces. The direct link to their respective jurisdictions may have been relatively limited, but in the wider interest of disrupting drug trafficking they worked on identifying online drug traffickers.<sup>26</sup>

Similar questions regarding the limits of jurisdiction and responsibility are also relevant when it comes to mutual legal assistance requests. One example is offered by the numerous large data hosting companies that have been established in the Netherlands.<sup>27</sup> Frequently, the Dutch authorities receive requests to seize or intercept servers with suspect data, such as online platforms that spread illegal content. Often, the requesting authority is only interested in one particular account, but it appears not always technically possible to single out that particular account. When executing the request, Dutch authorities may need to seize very

large volumes of data, and initial analyses often reveal that the seized data relates to crime all over the world. Hence, it is sometimes a challenge to determine who should obtain, process and act upon that data.

The example shows that solidarity is needed and the burden of work should be shared. Nevertheless, discussions on burden sharing are sometimes complex due to the differences in legal systems. For example, Dutch courts consider an extended conversation containing pictures or screenshots of money transfers sufficient evidence to convict a suspect of money laundering.<sup>28</sup> In other countries with different legal systems, the physical seizure of the money as well as the direct connection of that money with a crime is needed for conviction. Another example is the penalisation of inchoate crimes. The mere act of preparing a transport of cocaine is subject to a maximum sentence of six years in the Netherlands, whilst in other countries it is hardly worth being brought to court.<sup>29</sup>

It has been well-studied that significantly differing levels of penalties exist in EU Member States.<sup>30</sup> These stark differences in substantial criminal law limit the possibilities of sharing the burden of working together in cross-border crime in general, and data-driven investigations in particular.

##### 2. Obligation to share data and how the data was acquired

The jurisdiction of the investigating national authorities is commonly limited to crime occurring on its national territory or with a link to its territory. Their powers and resources may not legitimately be used for crimes that lie beyond that. Yet, there are many obligations in international treaties and positive human rights obligations to act if a serious crime is detected in another country.<sup>31</sup> Cooperation should not be rooted in a one-sided, particular interest of one state. The recently adopted Directive on exchange of information between the law enforcement authorities of EU Member States<sup>32</sup> does not encompass a direct obligation to share relevant information with foreign counterparts. But the spirit of loyal cooperation between EU Member States itself should inspire states to show solidarity when they suspect a crime to have occurred in another state.

When sharing data across borders, the issue of admissibility of that data as evidence merits additional consideration and collaboration.<sup>33</sup> When the encrypted communication server Exclu was recently hacked, the Dutch authorities shared an extensive package of national court orders and official reports that explain how the data was obtained. Yet, the standards for interception, data-processing, re-

cord-keeping, and transparency may be different in the receiving country. To meet the objective of sharing data in a reliable manner, it is necessary that the receiving public prosecutor or investigating judge explain their national requirements up front. In its judgment in *EncroChat*, the ECJ upheld the non-inquiry principle, while at the same time requiring that evidence be excluded if a person is not in a position to comment effectively on that information.<sup>34</sup> The interpretation of that last sentence will be subject to debate in many national courts in the coming years.

### 3. International data needs international context

(Automated) processing of large data volumes is a necessary step to select relevant data. In their attempt to select and understand data, national authorities cross-reference it against their own national databases. Hence, potentially relevant names and phone numbers from surrounding countries may easily slip through the cracks. This national focus seriously limits the scope of the analysis. There is empirical evidence that crime spread over different jurisdictions indeed prevents detection.<sup>35</sup> The need to include foreign data in the analysis is therefore obvious.<sup>36</sup> While jurisdictions regularly collaborate to collect relevant evidence, collaboration on storing and analysis is less common:<sup>37</sup> data is generally stored in accordance with national standards and analysed against national databases only.

The problem becomes evident, for example, when we look at the process of matching data between different Financial Intelligence Units (FIUs) within the EU.<sup>38</sup> The automated analysis of cross-border transactions by a national FIU is at most partial when foreign information on the persons involved in reported suspicious transactions cannot be included.

In our experience, it has proven of added value on several occasions to invite foreign analysts to a scrum session and both work on the same data set. Whilst this could be done as part of a Joint Investigation Team, the analytical teamwork as such can also take place within the framework of police cooperation. The data shared during such a session can be made subject to any conditions, including those from the applicable judicial warrants.<sup>39</sup>

Another challenge when processing content data is language. Naturally, our own teams of investigators principally speak Dutch as their native language. Yet, by focusing mainly on Dutch speakers and Dutch citizens we create our own blind spot. While working on the *EncroChat* and *SkyECC* data sets, we therefore actively sought cooperation with relevant foreign authorities to mitigate this effect and to prevent the bias of language. In practice, this meant

compiling top-ten lists of communication network users per nationality and actively approaching their respective country of origin with the aim of cooperation. This was a useful bottom-up approach, while the involvement of Europol had its advantages in distributing the analysis results.

The challenge to the selection and further processing of data is relevant also in the context of the principle of data minimisation. As already noted in relation to the national strategy on data-driven law enforcement (supra II), Art. 4(1) (c) of the LED requires that data only be processed in so far as it is relevant and not excessive. If the acquired data does not result in any matches, one may lightly conclude that the unmatched data is not relevant and may be deleted. Yet, if the data set has a strong cross-border component, that conclusion may only be reached once it has been sufficiently ensured that the legitimate interests of foreign jurisdictions have been met. Obviously, a data set of, for instance, participants in an online exchange of child pornography should not go undetected because the processing is limited to a particular jurisdiction. Likewise, a data set of internal communication of a foreign crime group may hold crucial evidence to solve serious crimes in another state.

### 4. Coordinating European criminal justice

A data-driven approach to tackling criminal networks is implemented effectively when trials against connected elements of the network can be carried out in various jurisdictions in a coordinated manner. The interest of justice is better served if the judicial authorities not only coordinate their initial efforts (who will prosecute?) but continue to stay in touch until the end of a trial.

For example, the conviction of a drug dealer/money launderer in Germany is likely to be relevant for the prosecution of the broker in the Netherlands. Likewise, a German judgment convicting an online drug trader who also sold drugs to Indonesia via the darkweb was later used in Dutch court proceedings as supporting evidence against the producer, in order to show the global distribution of his illicit products.<sup>40</sup>

Another example illustrating the need for coordination at the trial level are the *EncroChat/SkyECC* cases mentioned above. In the Netherlands, they have handed down well over 500 judgements to users of *SkyECC* and *EncroChat* to date.<sup>41</sup> Many of these judgements relate to conversations with criminals in other countries, or even include convictions for crimes committed abroad.<sup>42</sup> Whilst the EU framework calls for practitioners to contact each other when conflicts of jurisdiction arise, it is equally relevant to share milestones in related proceedings, including important statements, ac-



quittals, plea arrangements, and convictions. The sharing of the precise outcome of a court case can also be in the interest of the defence. An acquittal or different interpretation of the facts in one country should be known to the parties involved in related cases in other countries. Thus far it has proven difficult to be aware of relevant outcomes of EncroChat/SkyECC cases elsewhere in the EU. The automated exchange of criminal records through the ECRIS is insufficient: it is limited to final convictions,<sup>43</sup> whilst information on the earlier steps is equally relevant in practice.

## V. Conclusion

The surge of large data sets opens up opportunities for law enforcement to combat organised crime more effectively. Data-driven investigations are one way of achieving that. This article outlined that this approach is still a very new way of thinking in law enforcement, breaking with some of the traditional ways of starting and conducting investigations and allocating resources.

In the authors' experience, the close collaboration between the police and prosecution service has proven key to ensuring that data-driven investigations get off the ground and operate within the law. The correct application of the EU's

relevant data protection framework – the Law Enforcement Directive – is fundamental to that work, and it guarantees transparency to the defence and the court. However, some elements of the Law Enforcement Directive, such as the data minimisation principle and the requirement that only accurate data be processed, necessitate additional considerations when applied to large data sets.

We also demonstrated in this article that the cross-border nature of organised crime requires this data-driven work to be done in cooperation with international partners. As the criminals we investigate are digital nomads travelling the world, we have to foster a culture of digital cooperation as well. International law and solidarity require that data be shared proactively. Ideally, the burden of exploiting large data sets should be shared. And we must reflect on how to facilitate transparency and accountability at an early stage when we cooperate internationally on large data.

In addition, we have provided some insights into how the differences in substantial and procedural law within the EU make such conversations sometimes very complex. It will be interesting to further research the ratio of users versus convictions in the different EU Member States, and explore to what extent differences in substantive law play a role in the efficiency of criminal justice.

### Boudewijn de Jonge

Senior public prosecutor at the National Public Prosecution Office of the Netherlands.  
PhD candidate at the University of Leiden

### Barry de Vries

Inspector at the National Police of the Netherlands

\* The opinions in this article are strictly personal and do not necessarily reflect those of the organisations the authors work for. The authors thank Sarah Norman and Thomas Wahl of the eucrim team for their constructive comments on the earlier version of this article.

1 National Police of the Netherlands, Office of the Chief Commissioner, *Begroting en beheerplan 2024–2028* [Budget and management plan 2024–2028], 3 July 2023.

2 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.

3 The first initiatives to automatically match images go back to the year 2000. A. Minnaar, "An examination of early international and national efforts to combat online child pornography and child sexual exploitation and abuse material on the Internet", (2023) 24(2) *Child Abuse Research in South Africa*.

4 H. Goldstein, *Problem-Oriented-Policing*, 1990.

5 P.A.C. Duijn, *Detecting and disrupting criminal networks: A data driven approach*, 2016, [PhD thesis for the University of Amsterdam].

6 An excellent illustration of the application of this concept to countering cannabis cultivation is described in this movie: <<https://www.youtube.com/watch?v=Qhk9ciHlzzo>> accessed 6 January 2025.

7 Interesting work is done by Enderwick who compared regular multinational enterprises to criminal organisations. P. Enderwick, "Understanding cross-border crime: the value of international business research" (2019) 15(2/3) *Critical perspectives on international business*, 119–138.

8 European Monitoring Centre for Drugs and Drug Addiction and Europol, *EU Drug Market: Drivers and facilitators*, 2024.

9 InSight Crime and the Global Initiative Against Transnational Organized Crime, *The cocaine pipeline to Europe*, 2021; Organized Crime and Corruption Reporting Project, *The Highway to Europe – Inside A*

*Global Drug Collaboration*, 2023, available at <<https://www.occrp.org/en>> accessed 6 January 2025.

10 See for a more detailed description: E. van de Sandt, A. van Bunningen, J. van Lenthe and J. Fokker, *Towards Data Scientific Investigations: A Comprehensive Data Science Framework and Case Study for Investigating Organized Crime and Serving the Public Interest*, March 2021.

11 See for example: V. Harinam and B. Ariel, "The Role of Law Enforcement in the Regulation of Cryptomarkets (and the Limited Role of Deterrence)", in: *Law Enforcement Strategies for Disrupting Cryptomarkets: A Practical Guide to Network Structure, Trust Dynamics, and Agent-Based Modelling Approaches*, 2024, pp. 49–83.

12 M. den Hengst, and O.L. Wijsman, "Datagedreven politiewerk: Een organisatorisch en juridisch perspectief", in: T. Snaphaan, W. Hardyns, A. J. van Dijk, R. Spithoven and R. Van Brakel (eds.), *Big data policing*, 2023, pp. 71–90.

13 Art. 4(1)(d) of the LED, *op. cit.* (n. 2).

14 For instance: Court of Amsterdam, 27 February 2024, ECLI:NL:RBAMS:2024:692.

15 The EU framework for forwarding of data to a new investigation depends on whether the data was (a) collected from telecom providers or (b) collected by the authorities (see also the conclusion in Case C-162/22 by Advocate General Campos Sánchez-Bordona, ECLI:EU:C:2023:266, paras. 41–45). In the first scenario, data may only be forwarded if the receiving investigation concerns a serious crime or serious threat to public security (ECJ, 7 September 2023, Case C-162/22, *Lietuvos Respublikos generalinė prokuratūra*, ECLI:EU:C:2023:631, summarized at *eucri* [2/2023, 149–150](#)). In the second scenario, data obtained legitimately may be processed for other criminal investigations, in accordance with national law.

16 Court of The Hague, 19 March 2021, ECLI:NL:RBDHA:2021:3224.

17 The ECtHR accepts that the defence counsel may be granted access to a limited data set, but must be granted full access to relevant material: ECtHR, 4 June 2019, *Sigurður Einarsson v Iceland*, Appl. no. 39757/15.

18 See on this matter, for instance: ECtHR, 25 July 2019, *Rook v Germany*, Appl. no. 1586/15.

19 See <[www.hansken.nl/hansken-academy/hansken-courses/hansken-for-lawyers](http://www.hansken.nl/hansken-academy/hansken-courses/hansken-for-lawyers)> accessed 6 January 2025. For an example on how the defense uses the system, see: Court of Amsterdam, 1 April 2021, ECLI:NL:RBAMS:2021:1507.

20 I. Helsloot, P. van Lochem, C. Kijne, "Slimme(re) Opsporing. Een verslag van de ontwikkeling en pogingen tot implementatie van een handreiking voor efficiënte opsporing door de politie", (2022) *Politiewetenschap*, 125.

21 For an explanation and overview of the efforts to counter underground banking, see: Annual Review Criminal Money Flows 2022, Public Prosecution Service of the Netherlands, 2 April 2023, available at: <<https://www.prosecutionservice.nl>> accessed 6 January 2025.

22 One example is the conviction of an underground banker who moved €246 million by the court of Rotterdam on the basis of SkyECC data: Court of Rotterdam, 5 September 2024, ECLI:NL:RBROT:2024:8533.

23 A system based on the legality principle may have to make different choices. The massive launch of large criminal cases due to EncroChat forced the government of Hamburg to assign 28 additional judges, prosecutors and judicial staff in 2021: Senat Hamburg, Press release of 1 June 2021, <<https://www.hamburg.de/politik-und-verwaltung/behoerden/bjv/aktuelles/presse-meldungen/2021-06-01-bjv-en-crochat-ermittlungen-232564>> accessed 6 January 2025.

24 B. de Jonge, "Transnational Crime Without Transnational Prosecution: How Positive Obligations to Cooperate May Inspire National Judicial Authorities", (2023) 2(2) *Transnational Criminal Law Review*, 98–112.

25 The lack of such rules is particularly noticeable in the context of

digitalized crime. See for instance: T. Beekhuis, "Executieve jurisdictie: het (grote) obstakel in grensoverschrijdende opsporingsonderzoeken naar (gebruikers van) cryptoaanbieders?", (2022) *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 106–118.

26 Over the years, the German authorities have taken down dark-web marketplaces, such as Crimenetwork (2024), Nemesis (2024), Kingdom (2023), Hydra (2022) and Wall Street (2019). These marketplaces were used by hundreds of vendors and visited by thousands of buyers around the globe.

27 To avoid any misunderstandings: the reason why many companies host large datacenters in the Netherlands has to do with the proximity of transatlantic sea cables, availability of qualified staff, and general economic climate.

28 The decision of 12 July 2022 by the Court of The Hague, ECLI:NL:RBDHA:2022:6763, exemplifies Dutch case law. Here, the court found the combination of a picture of bank notes and the message that "it was 428" sufficient proof that the suspect was laundering €428,000.

29 Court of The Hague, 24 December 2021, ECLI:NL:RBDHA:2021:14242.

30 EMCDDA, *Drug trafficking penalties across the European Union a survey of expert opinion*, Lisbon 2017, pp. 15–23. For a critical overview of the efforts to harmonise sanctions within the EU, see for instance: K. Zoumpoulakis, "Approximation of criminal sanctions in the European Union: A wild goose chase?", (2022) 13(3) *New Journal of European Criminal Law*, 333–345.

31 Both treaty law (the crime control treaties) and human rights case law include multiple specific obligations to cooperate when authorities are faced with cross-border crime. See *supra* note 24.

32 Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA, OJ L 134, 22.5.2023, 1.

33 The principle of non-inquiry may be a strong principle in several EU Member states, but its interpretation is subject to debate. See G. Sagittae, "On the lawfulness of the EncroChat and Sky ECC-operations" (2023) 14(3) *New Journal of European Criminal Law*, 273.

34 ECJ, 30 April 2024, Case C-670/22, *M.N. v. Staatsanwaltschaft Berlin (EncroChat)*, summarised in *eucri* [1/2024, 40–43](#).

35 M. Lammers and W. Bernasco, "Are mobile offenders less likely to be caught? The influence of the geographical dispersion of serial offenders' crime locations on their probability of arrest", (2013) 10(2) *European Journal of Criminology*, 168–186.

36 D. Skillicorn, *Cyberspace, data analytics, and policing*, 2022, p. 234.

37 As shown by Den Hengst, and Wijsman, *op. cit.* (n. 12), p. 27.

38 F. Mouzakiti, "Cooperation between financial intelligence units in the European Union: stuck in the middle between the general data protection regulation and the police data protection directive", (2020) 11(3) *New Journal of European Criminal Law*, 351–374.

39 Art. 3 lit. c) of Directive (EU) 2023/977, *op. cit.* (n. 32).

40 Court of Appeal of The Hague, 1 February 2022, ECLI:NL:GHDHA:2022:346.

41 This number is based on the judgements of first instance courts published on the official webpage of the Dutch judiciary: <[www.rechtspraak.nl](http://www.rechtspraak.nl)>. The real number should be higher, because there is no general obligation to publish every judgement.

42 Dutch law established broad extraterritorial jurisdiction over Dutch nationals committing crimes abroad, and over foreign nationals if they contribute to a criminal organisation that can be prosecuted in the Netherlands.

43 Art. 2 of Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93, 7.4.2009, 23.

# A Plea for Common Standards on the Lawyer-Client Privilege in EU Cross-Border Criminal Proceedings in Light of Advancing Digitalisation

Lorena Bachmaier Winter\*

While the right to lawyer-client confidentiality has long been recognised as a fundamental right enshrined in the right to legal assistance and the right of defence, its practical implementation does not seem to provide adequate safeguards. Many EU Member States still lack clear rules on how to ensure that privileged communications are not captured during the interception of communications and the search/seizure of computers during criminal investigations. Also, OLAF investigations struggle with deficiencies in safeguarding the lawyer-client privilege. Taking the case law of the European Court of Human Rights as a starting point to identify common standards on the lawyer-client privilege in criminal proceedings, this article argues that there is a need for the European Union to take legislative action to ensure the effective protection of this right.

## I. Introduction

The Charter of Fundamental Rights of the European Union (CFR) and the European Convention on Human Rights (hereinafter: ECHR or the Convention) do not expressly guarantee the defendant's right to communicate confidentially with his/her defence attorney. However, this right is enshrined in the fair trial safeguards of Arts. 47 and 48 CFR and in Art. 6 ECHR. The ECtHR has been very attentive when it comes to protecting this right, and the content and scope of the right to lawyer-client confidentiality has been continuously clarified in its case law. The Court of Justice of the European Union (CJEU) has addressed the lawyer-client privilege and legal professional secrecy only in few judgments so far,<sup>1</sup> which is why ECtHR case law is paramount for defining EU common standards on this matter.

The Strasbourg Court has repeatedly declared that the lawyer-client privilege and the confidentiality of their communications is the basis of the relationship of trust that must exist between the lawyer and his/her client. It has also stressed that this privilege is one of the core elements of the right to a fair trial in a democratic society.<sup>2</sup> This right is set out in Art. 6(3) lit. c) ECHR and covers face-to-face/oral communications, as well as communications by post or by telephone, or by way of any electronic system. In addition, the ECtHR stressed that the safeguarding of professional secrecy is the corollary of the right to legal assistance and the right against self-incrimination.<sup>3</sup> Any interception of the communications between lawyer and client in criminal proceedings falls within the scope of private life and implies an interference with Art. 8 ECHR, which can also entail an

infringement of Art. 6 ECHR.<sup>4</sup> The protection of the confidentiality of these privileged communications has become even more challenging in the digital environment, in which law enforcement access to electronic data and communications is likely to be done without filtering these communications.

While certain common standards have been set out by the ECtHR, there are still important differences in the protection of the right to lawyer-client confidentiality at the national level.<sup>5</sup> Such asymmetries within the EU entail important risks in transnational criminal proceedings and may lead to violations of this right in the context of cross-border evidence gathering. Taking the example of investigations into offences detrimental to the EU's financial interests, it can be seen that there is further a lack of precise provisions for the digital investigative operations carried out by OLAF, despite the high standards on digital forensics.<sup>6</sup> Against this background, this article makes a plea for the protection of the lawyer-client privilege at the European Union level. It explores specific safeguards for the access of data that might contain privileged communications.

To advance towards an EU legislative framework, it is important to first take stock of the content of the right to the lawyer-client privilege as defined by the ECtHR in its case law.<sup>7</sup> I will summarise the ECtHR's case law on certain investigative measures, precisely on access to and interception of communications of lawyers; entry and search of lawyers' offices and computers; and access to electronic data, since these are measures that entail a high risk of violating the lawyer-client privilege.<sup>8</sup> After

reviewing the standards defined by the Strasbourg Court, I will point out some of the problems that might emerge in cross-border criminal proceedings in the area of freedom, security and justice, not only as regards the protection of the lawyer-client privilege in OLAF's digital investigations, but also when executing a European Investigation Order (EIO) and within the context of the future application of the Regulation on the European Production and Preservation Orders for electronic evidence. Lastly, I will argue in my conclusions that European Union law should comprehensively address the protection of the right to lawyer-client confidentiality in transnational criminal proceedings to effectively ensure the right of defence and also to prevent problems regarding the admissibility of cross-border criminal evidence.

## II. Overview of the ECtHR Case Law on the Lawyer-Client Privilege in Criminal Investigations

The protection of the lawyer-client privilege is recognised in several recommendations of the Council of Europe's Committee of Ministers and Parliamentary Assembly.<sup>9</sup> In addition, the United Nations adopted in 1990 the Basic Principles on the Role of Lawyers.<sup>10</sup> The ECtHR developed several principles on the lawyer-client privilege, which can be summarised as follows:

- Any person who wishes to consult a lawyer should be free to do so under conditions which favour full and uninhibited discussion;<sup>11</sup>
- The protection of confidentiality is not limited to the protection of communications or actions related to pending proceedings;<sup>12</sup>
- The right to confidentiality of lawyer-client communications must be guaranteed in such a way that its exercise is effective and not merely formal.<sup>13</sup>

The ECtHR differentiates between interferences in conjunction with the right of Art. 8 ECHR (right to respect for private life and correspondence) because of measures adopted in the context of a criminal investigation, on the one hand, and the impact that the violation of the right to the lawyer-client confidentiality may have on the rights guaranteed under Art. 6 ECHR, on the other.<sup>14</sup> The seizure of a client's documents that are in the possession of his/her lawyer and that are obtained without respecting the right to professional secrecy, can also constitute a violation of the right against self-incrimination.<sup>15</sup>

Since *Golder v. United Kingdom*<sup>16</sup> and *Niemietz v. Germany*,<sup>17</sup> the Court has been defining the requirements that must be met so that interference in the lawyer-client privilege can

be considered to be in accordance with the Convention.<sup>18</sup> These requirements are analysed when addressing the different investigative measures.

### 1. Interception of telephone communications

The right to defense and legal assistance would not be effective without the protection of the confidentiality of lawyer-client communications. Although not all conversations between the lawyer and his/her client are protected by the lawyer-client privilege, all European legal systems strictly prohibit intercepting the telephone of a lawyer who is not suspected or charged with a criminal offence, because Art. 8 ECHR protects the confidentiality of any "communication" and in addition grants a reinforced protection to communications between lawyers and their clients.<sup>19</sup> In practice, the major problem arises from communications that are accidentally intercepted when the defendant's telephone is tapped or his/her computer searched.<sup>20</sup> Indeed, there is consensus that it is almost impossible to prevent some of these conversations from being overheard or even recorded, and the ECtHR has put the focus on the need for a legal regulation providing for adequate safeguards, such as the destruction of the recordings.<sup>21</sup> However, the Court has not gone so far as to impose an exclusionary rule of evidence on the states.<sup>22</sup>

### 2. Entry, search and seizure: Specific requirements for seizing computer files of lawyers and in law offices

Most legal systems only authorise the entry and search of a law firm and its files and computers, when the lawyer himself/herself is the suspect of a crime,<sup>23</sup> but there are still many countries that will allow this measure even if the lawyer is not the suspect. The ECtHR takes a much stricter approach if the search is carried out in the office of a lawyer who is not a suspect,<sup>24</sup> requiring "compelling reasons" to justify such interference in Art. 6 and eventually Art. 8 ECHR.<sup>25</sup> The ECtHR has accepted such measures if there is an adequate and sufficient legal provision, namely if the objective pursued is legitimate and meets the requirement of necessity and proportionality, and the search can be carried out respecting the adequate safeguards.<sup>26</sup>

#### a) Safeguards developed by the ECtHR

In the case law of the Court, most judgments that have found a violation of Art. 8 ECHR were based on the lack of a sufficient legal provision and, specifically, because the legal framework did not provide for specific safeguards to protect lawyer-client confidentiality.<sup>27</sup> According to

the Court,<sup>28</sup> the national law must specify who shall execute the measure and how the search and seizure shall be carried out, including detailed rules on how electronic data related to the crime under investigation should be accessed and what safeguards are in place to avoid abusive searches and the seizing of privileged files. If such legal safeguards are in place, the Court proceeds to check whether they have been effectively implemented during the search and seizure of the lawyer's office. The ECtHR, in particular, has paid special attention to the following two circumstances:

1. Whether the judicial warrant is issued upon reasonable suspicion and whether the scope of the search and seizure is limited

This is not a mere formality;<sup>29</sup> in order to comply with the Convention, the scope of the search and seizure must be clearly limited, especially when it comes to computer searches and access to electronic files in order to ensure the principle of proportionality.<sup>30</sup> The ECtHR noted that, where a court order allows the search and seizure of all personal computers and data storage devices without limiting the search to those files likely to contain evidence and be relevant to the ongoing criminal investigation, such broad authorisation is not compatible with the guarantees that must be respected in order to protect professional secrecy, therefore constituting a violation of Art. 8 ECHR.<sup>31</sup>

2. Whether sufficient safeguards were adopted to protect professional secrecy during the search and seizure

Some of the safeguards the ECtHR has taken into account when assessing possible violations of the Convention, include the following:<sup>32</sup>

- A procedure for separating privileged documents/material, so that they are not seized;
- Measures to prevent officers from accessing the privileged documents/material;
- The search is carried out in the presence of the lawyer and he/she has the chance to identify any documents/material protected by the right to confidentiality and to ensure that the number of seized elements is not disproportionate;
- The presence of an independent observer who can monitor that files protected by professional secrecy are not seized.
- In some cases, as a reinforced safeguard, the presence of a judge during the search, who supervises that it complies with the court order.<sup>33</sup>

The ECtHR considers the presence of an independent third party with sufficient qualifications to ensure that documents/material protected by professional secrecy are not

seized an important safeguard for the conformity of the entry and search of a law firm, in line with the Convention and therefore an almost absolute requirement.<sup>34</sup> However, the presence of the lawyer and two witnesses was not considered sufficient in a number of cases.<sup>35</sup>

As to the safeguards that need to be in place in order to protect files and communications subject to the lawyer-client privilege, the Court has laid down guidelines regarding the search and seizure of computers and electronic files.<sup>36</sup>

## b) Problems in practice and the ECtHR's reaction

The investigative measures of search and seizure of computers and electronic files continue to pose problems in practice, since most legal systems do not include detailed rules on how the measures should be executed. The judicial warrant authorising the search and seizure often only specifies the type of documents that can be sought and seized but not the keywords or search programmes to be used to identify the files protected by the lawyer-client privilege. The case of *Wolland v. Norway*<sup>37</sup> is interesting in this respect, as it shows the detailed procedure to be followed according to Norwegian law in cases of computer searches as well as all the safeguards provided to prevent privileged documents and communications from being accessed and seized.<sup>38</sup>

Furthermore, although on-site searches should be the rule, this is not always feasible, and it is common practice for police officers to seize all the hardware and computers and move them to designated premises in order to carry out the examination by public IT officers or independent computer experts in a forensic laboratory.

In the case of *Sārgava v. Estonia*, which dealt with the search of electronic devices of lawyers, the ECtHR made a very clear statement on the need to separate the files protected by the lawyer-client privilege and that this safeguard is of utmost importance when it comes to electronic data and searches of electronic devices:<sup>39</sup>

While the question of sifting and separating privileged and non-privileged files is undoubtedly important in the context of hard copy material, it becomes even more relevant in a situation where the privileged content is part of larger batches of digitally stored data. In such a situation, even if the lawyer concerned or his representative is present at the search site, it might prove difficult to distinguish swiftly during the search which exact electronic files are covered by legal professional privilege and which are not.

The question of how to carry out sufficiently targeted sifting is equally pertinent in circumstances where under domestic law or practice such sifting is not carried out at the



site of the search, but the data carriers are instead seized in their entirety and/or a mirror-image copy of their content is made. The Court has acknowledged that cloning the devices might be necessary to prevent illicit data tampering with the device. It has also allowed the devices to be quickly returned to their owner(s) but required measures to be adopted to guarantee that, during the copying and screening of the content of the devices, data not covered by the judicial authorisation and privileged data are not accessed or seized.<sup>40</sup>

In *Sārgava v. Estonia*, the Court found a violation of the Convention, taking into account the following:<sup>41</sup> the judicial order did not specify the measures to be adopted in order to protect professional secrecy, even though it was already known that protected documents were stored on the seized devices; the national law neither established the procedure to be followed to access electronic data nor did it contemplate specific measures guaranteeing that the protection of professional secrecy would be guaranteed during the examination of the devices; the person under investigation neither participated in nor was present during the selection of the search terms and files to be examined in the criminal proceeding. This case is highly relevant, because, according to the ECtHR, the absence of a legal regulation with specific provisions on the handling of electronic files and the sifting through of privileged documents already constitutes a violation of Art. 8 ECHR, even if, in practice, the measure was executed respecting the principle of proportionality after a sound perusal of the files.

In conclusion, for the Court, the absence of a clear procedural scheme that defines how the search of electronic devices must be carried out with full guarantees, and the fact that the law does not establish safeguards to prevent the privileged documents from being downloaded and read by investigators once the computers have been seized, entails a breach of the Convention.<sup>42</sup>

### III. Lawyer-Client Privilege and the Cross-Border Gathering of Evidence in the EU

Looking first at the lawyer-client privilege in investigations related to the protection of the EU's financial interests, there is a complete set of guidelines to be followed in digital forensic procedures carried out by OLAF: Guidelines on Digital Forensic Procedures for OLAF Staff.<sup>43</sup> These guidelines not only provide for technical standards but also for legal standards to ensure defence rights and also compliance with the principle of proportionality. With regard to the pro-

tection of privileged material, the guidelines set out that if, during an "on-the-spot check" operation, the representative of the economic operator claims that the device being inspected contains legally privileged data, such data is to be acquired and placed in a sealed envelope.<sup>44</sup> Furthermore, the guidelines provide that, before opening the envelope, the economic operator "will be invited for a meeting to resolve the issue". To this end, he/she may be assisted by a person of his/her choice.

This safeguard is adequate to prevent the lawyer-client privilege – and other privileged materials – from being infringed during the collection of digital evidence; providing for the entity's representative to be present while the data are analysed and/or sifted is also a positive measure. However, such provisions are not sufficient to effectively protect the lawyer-client privilege, since the guidelines do not establish how the sifting is to be done. To prevent disclosure and access to privileged data, more detailed provisions would need to be adopted in order to ensure that the OLAF investigation report is not excluded as evidence in a subsequent criminal procedure.

Looking second at accessing cross-border evidence within the EU, the following paragraphs will deal with two EU instruments: the Directive on the European Investigation Order (hereinafter DEIO)<sup>45</sup> and the Regulation on European Production and Preservation Orders for electronic evidence (hereinafter EPO/EPRO-Regulation).<sup>46</sup>

#### 1. The European Investigation Order

The DEIO is based on the principle of mutual recognition, nonetheless providing a quite extensive list of refusal grounds (mainly, but not exclusively, stipulated in Art. 11). This scheme introduces some flexibility in the execution of an EIO and avoids "blind" recognition, which might be contrary to procedural principles and safeguards. Among the refusal grounds, Art. 11(1) DEIO lists the existence of an immunity or a privilege under the law of the executing state.<sup>47</sup>

Very frequently, the breach of the lawyer-client privilege occurs by way of accidental interceptions of the communications or documents of the suspect or a third person, thus cases in which the lawyer or his/her offices and electronic devices are not the target. In practice, these interferences into the right to lawyer-client confidentiality are almost impossible to avoid and hence the protection of this right needs to be done *ex post*, by preventing such material from reaching the trial and/or being used as evidence. As a rule, the grounds for refusal for executing the EIO would not play

a role here, because the accidental interception of privileged communications can neither be foreseen nor avoided beforehand.

Other means of access to privileged files and communications of a lawyer in execution of an EIO can be: during the entry and search of the lawyer's office; and accessing the lawyers' computers or other digital devices (remotely or located outside the office). In principle, such measures are not to be refused if they are provided for in the executing state for similar cases.

However, the most problematic question relates to the way in which the search and seizure of documents/data should be carried out, so that the executing state respects its own procedural rules on protection of privileged material and, at the same time, complies with the *lex fori* to ensure that the evidence gathered will be admissible as evidence. There is no legal harmonisation on how to proceed with regard to the safeguards for filtering privileged and non-privileged files/communications.

Furthermore, the exclusionary rules of evidence among the EU Member States also differ from each other, and thus the effective protection of the lawyer-client privilege might become completely ineffective if, for example, the seized electronic files are not filtered in the executing state and the privileged communications are not excluded as evidence in the forum state. The problems deriving from the absence of common rules on the admissibility of evidence in criminal proceedings have been pointed out numerous times:<sup>48</sup> as long as the evidentiary rules are not adequately harmonised among the different Member States, the transfer of evidence from one country to another will impact the level of procedural safeguards and the rights of the defence.<sup>49</sup> The issue that arises here is how to protect the fundamental right to the confidentiality of lawyer-client communications when executing an EIO? Which system of sifting the data should be in place? Who should control it? Should the filtering of data be carried out *in situ*? If so, according to which rules? What happens when the EIO defines the scope of the search and the type of data to be seized but does not specify the keywords to be used or the way in which the data should be sifted to prevent unlawful interference into the right to lawyer-client confidentiality?

Problems arise if the executing authority has adopted its own protocols for separating the privileged materials, but these are not provided in a legal provision and thus might not be in accordance with ECtHR case law. Would the evidence obtained in such a way, lacking a sufficient legal basis in the executing state and thus being in breach of the

ECtHR, be admissible as evidence in the forum state? The general rule is that, if the *lex loci* has been complied with, the evidence should be admissible unless the evidence has been obtained in violation of human rights. And, according to the ECtHR, if safeguards to prevent interference with the lawyer-client privilege were not sufficiently regulated in the (national) law, the ECHR has not been complied with.

If the issuing state requires the executing state to exclude privileged information, but the issuing authority nevertheless receives privileged data, how should this situation be dealt with? Should the receiving authority simply exclude them and carry out the sifting in the issuing state, or would this circumstance already lead to a violation of the lawyer-client privilege?

Indeed, when the files seized include materials or communications covered by the lawyer-client privilege, it would mean that the safeguards to prevent such a violation were not adequate or not adequately implemented when carrying out the search and seizure. The lack of safeguards or non-compliance with them would amount to a breach of the Convention according to the ECtHR case law described above.

Lastly, the issuing authority might request the complete cloning of a computer in the executing state and the sending over of the complete data to be filtered according to the laws of the forum. The ECtHR has admitted that the quantity of the files searched and seized is not *per se* contrary to the Convention if there are adequate counterbalancing safeguards in place to protect the right to lawyer-client confidentiality. In this case, what would be the counterbalancing measures to be checked?

## 2. European Production Order for e-evidence

With regard to the rules for protecting the lawyer-client privilege in the context of access to electronic data by way of a European Production Order (EPO),<sup>50</sup> the relevant safeguards are provided in Art. 5 EPO/EPRO-Regulation. The Regulation implies the following principle:<sup>51</sup>

[I]t should be possible for the enforcing authority, where it is notified pursuant to this Regulation, to refuse a European Production Order where the data requested are protected by immunities or privileges granted under the law of the enforcing State which prevent the execution or enforcement of the European Production Order [...].

As regards the safeguards for privileged data, the Regulation distinguishes between two situations. The first situation is found in Art. 5(9) EPO/EPRO-Regulation, which reads as follows:

In cases where data protected by professional privilege under the law of the issuing State are stored or otherwise processed by a service provider as part of an infrastructure provided to professionals covered by professional privilege ('privileged professional'), in their business capacity, a European Production Order to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in Art. 3, point (10), or to obtain content data may only be issued:

- (a) where the privileged professional resides in the issuing State;
- (b) where addressing the privileged professional might be detrimental to the investigation; or
- (c) where the privileges were waived in accordance with the applicable law.

This provision seeks to protect the professional privilege, first by way of preventing the issuing of an EPO to obtain traffic (save for identification of the user) and content data of a lawyer, requiring the issuing authority to check (1) whether the lawyer resides in the forum state; or (2) whether the data cannot be obtained directly from him/her (because this would be detrimental to the investigation); or (3) whether the privilege has been waived. In any event, once the EPO has been issued to request traffic or content data, the authority (judge) of the enforcing state who is to be notified (Art. 8 EPO/EPRO-Regulation) will also have to check whether these conditions are met.

The second paragraph of Art. 5(10) EPO/EPRO-Regulation establishes that, if the issuing authority has "reasons to believe" that the traffic or content data requested are protected by professional privilege under the laws of the enforcing state, it shall not issue the EPO –and, if issued, in accordance with Art. 12 (1) (a) the authority in the enforcing state can invoke a ground for refusal.

This provision prevents Internet Service Providers (ISPs) as addressees from enforcing the EPO if the requested traffic or content data are protected by the lawyer-client privilege in the enforcing state. Of course, an ISP is not expected to check this, since it would be almost impossible to do so. Therefore, the Regulation relies on the proper examination by the issuing authority when sending out such an EPO, namely that it has "reasons to believe" that such data are covered by legal privilege.

In contrast to the EIO, Art. 5 (9) and (10) of the EPO/EPRO-Regulation is not based on mutual recognition but on prohibiting cross-border cooperation to access traffic or content data that are privileged under the *lex loci*. This mechanism is clearly more restrictive than the applicable rules under the EIO – where the privilege might be invoked as a ground for refusal: the Regulation states that privileged data are not subject to being accessed by an issuing authority by way of an EPO if they are also protected in the

enforcing state. Since the lawyer-client privilege is protected in all EU states, an EPO cannot be issued to obtain traffic or content data covered by the Regulation. However, if the issuing authority does not have "reasons to believe" that the data requested are privileged, and the EPO complies with requirements under Art. 5 (9) EPO/EPRO Regulation, it will be up to the notified authority in the enforcing state to check this circumstance after issuance of the EPO (Art. 8 EPO/EPRO Regulation). This is problematic, because it will be difficult for the authority in the enforcing state to notice this if the issuing state does not point out some form of possible professional privilege.

In sum, the implementation of the rules provided in the EPO/EPRO-Regulation relies completely on the assessment of the issuing state ("reasons to believe") in that the EPO affects data protected by professional privilege. As a rule, neither the ISP nor the authority in the enforcing state will be able to check whether the data requested effect a legal privilege if the issuing authority does not provide any hints in this direction. And while Art. 18 EPO/EPRO-Regulation regulates the right to an effective judicial remedy, this will only be activated *ex post*. It is doubtful whether this scheme will afford sufficient protection if the national rules do not provide for an exclusionary rule of evidence in case of breach of the lawyer-client privilege.

#### IV. Conclusion

While the right to lawyer-client confidentiality has long been recognised as a fundamental right enshrined in the rights to legal assistance and of defence, its practical implementation does not seem to provide adequate safeguards. As outlined in this article, OLAF investigations seek to protect this privilege, but neither its legal framework nor its guidelines include sufficient safeguards; and many EU Member States still lack clear rules on how to ensure that privileged communications are not captured during the interception of communications and the search/seizure of computers. The digitalisation of society and its communications has heightened the need to implement specific safeguards to prevent unlawful access to materials protected by professional secrecy through investigative measures that breach this protective right. As seen above, the ECtHR has called for the provision of specific rules to prevent overly intrusive access to lawyer-client privileged files and communications.

Identifying the standards for protection of the fundamental right to confidentiality of the lawyer-client relationship is only the first step in future legislation on the protection of the lawyer-client privilege in criminal proceedings at the EU

level – by way of a future Directive. It is not only sufficient to draw attention to the need to ensure the protection of the lawyer-client privilege; this right should also be effectively protected in the cross-border gathering of criminal evidence, especially when accessing both electronic storage devices and electronic data held by internet service providers. This article has particularly demonstrated that

the rules enshrined in the Directive relating to the European Investigation Order and in the Regulation on e-evidence (EPO/EPRO-Regulation) are not sufficient to grant effective protection. It is a plea for a European legislative framework laying down common standards on the lawyer-client privilege in cross-border criminal proceedings. In my opinion, supranational legislative action is absolutely needed.



**Prof. Dr. Lorena Bachmaier Winter**  
Full Professor of Law, Complutense  
University Madrid (UCM), Spain

\* This article elaborates on previous findings and publications by the author on the topic of the lawyer-client privilege. It was written within the framework of the research project «Proceso penal transnacional, prueba y derecho de defensa en el marco de las nuevas tecnologías y el espacio digital» (PID2019-107766RB-I00), financed by the Spanish Ministry of Science and Innovation.

1 E.g., CJEU (Grand Chamber), 8 December 2022, C-694/20, *Orde van Vlaamse Balies*; CJEU, 26 September 2024, Case C432/23, *Ordre des avocats du barreau de Luxembourg*. Both decisions deal with preliminary references related to the administrative cooperation in the field of taxation and the application of Directive 2011/16/EU.

2 See, for example, ECtHR, 28 November 1991, *S. v. Switzerland*, Appl. nos. 12629/87 and 13965/88, para. 48.

3 On the lawyer-client privilege in the USA, see the comprehensive reference book by E. Epstein, *The Attorney-Client Privilege and the Work-Product Doctrine*, ABA Publishing, Chicago, 2017.

4 On this issue, see generally T. Spronken and J. Fermon, “Protection of Attorney-Client Privilege in Europe”, (2008) 27 *Penn State International Law Review*, 439–463.

5 For a broad comparative law approach, see L. Bachmaier Winter, S. Thaman, and V. Lynn, (eds.), *The Right to Counsel and the Protection of Attorney-Client Communications in Criminal Proceedings. A Comparative View*, 2020.

6 See the “Guidelines on Digital Forensic Procedures for OLAF Staff”, 15 February 2016, accessible at: <[https://anti-fraud.ec.europa.eu/document/download/87e5deb1-8a64-42ca-8e08-234355dbe544\\_en?file\\_name=guidelines\\_en\\_bb84583638.pdf](https://anti-fraud.ec.europa.eu/document/download/87e5deb1-8a64-42ca-8e08-234355dbe544_en?file_name=guidelines_en_bb84583638.pdf)> accessed 11 October 2024.

7 On this topic, see L. Bachmaier, “Lawyer-client privilege en la jurisprudencia del Tribunal Europeo de Derechos Humanos”, in: L. Bachmaier (ed.), *Investigación penal, secreto profesional del abogado, empresa y nuevas tecnologías. Retos y soluciones jurisprudenciales*, 2022, 21–79.

8 It would go beyond the scope of this article to address the issue of who the owner of the right to professional secrecy is and who can waive the right to the lawyer-client privilege. On this issue, see

the highly debated ECtHR case *Klaus Müller v. Germany*, Appl. no. 24173/18, 19 November 2020. Analysing the problems related to execution orders in administrative taxation proceedings, which have been addressed by the CJEU, also exceeds the scope of this article. Nevertheless, it is important to underline that the CJEU has found it to be in violation of Art. 52(1) CFR if, under national law, a lawyer in tax matters does not benefit from the enhanced protection of communications between a lawyer and his client as guaranteed by Art. 7 CFR, except where there is a risk of criminal prosecution for the client (see CJEU, 26 September 2024, Case C432/23, *op. cit.* (n. 1)).

9 See mainly Recommendation No. R(2000)21 on the freedom of exercise of the profession of lawyer (adopted by the Committee of Ministers of the Council of Europe on 25 October 2000); Parliamentary Assembly, Recommendation Rec 2085 (2016) of 28 January 2016, *Strengthening the protection and role of human rights defenders in Council of Europe Member States*; see also No. 93 of the Appendix to the *Standard Minimum Rules for the Treatment of Prisoners*, Resolution (73) 5 of the Committee of Ministers of 19.1.1973.

10 *Basic Principles on the Role of Lawyers* adopted on 7 September 1990, ONU Doc. A/CONF.144/28/Rev.1 p. 118 (1990), para. 22.

11 ECtHR, 25 March 1992, *Campbell v. United Kingdom*, Appl. no. 13590/88, para. 46. On the impact of the ECtHR’s case law and the lawyer-client privilege in common law systems, see J. Auburn, *Legal Professional Privilege: Law and Theory*, 2000, pp. 37 ff.

12 See ECtHR, 9 April 2019, *Altay v. Turkey* (No. 2), Appl. no. 11236/06, paras. 49–51.

13 See, for example, ECtHR, 27 April 2017, *Sommer v. Germany*, Appl. no. 73607/13, para. 56; ECtHR, 6 December 2012, *Michaud v. France*, Appl. no. 12323/11, para. 130. This requires providing specific measures and safeguards to ensure such effective protection.

14 See ECtHR, 21 February 1975, *Golder v. United Kingdom*, Appl. No. 4451/70, para. 45; ECtHR, 25 July 2017, *M. v. The Netherlands*, Appl. no. 2156/10, para. 85. In the latter case, the ECHR deals with the possible violation of Art. 6(3) lit. c) ECHR in a matter related to the disclosure of classified information and the restrictions on access to a lawyer and communication confidentially in the context of facts involving state secrets and national security interests.

15 See ECtHR, 24 July 2008, *André and Another v. France*, Appl. no. 18603/03, para. 41. However, in its assessment, the Court usually does not enter into analysing the infringement of Art. 6 ECHR once it has confirmed that there was a violation of Art. 8 ECHR.

16 *Op. cit.* (n. 14).

17 ECtHR, 16 December 1992, *Niemietz v. Germany*, Appl. no. 13710/88.

18 The ECtHR has also extensively addressed the right of the detainee to communicate with their lawyer as a substantial part of the right to defence and the right to legal assistance. See, e.g., ECtHR, *Golder v. United Kingdom*, *op. cit.* (n. 14); ECtHR, 20 June 1988, *Schönberger*



- and *Durmaz v. Switzerland*, Appl. No. 11368/85; ECtHR, 13 March 2007, *Castravet v. Moldova*, Appl. no. 23393/05; ECtHR, 4 October 2005, *Sarban v. Moldova*, Appl. no. 3456/05; ECtHR, 31 May 2011, *Khodorkovskiy v. Russia*, Appl. no. 5829/04; ECtHR, 24 May 2018, *Laurent v. France*, Appl. no. 28798/13.
- 19 ECtHR, 27 October 2015, *R.E. v. United Kingdom*, Appl. no. 62498/11, para. 131; or ECtHR, 7 November 2017, *Dudchenko v. Russia*, Appl. no. 37717/05, para. 104.
- 20 L. Bachmaier Winter, “Intervenciones telefónicas y derechos de terceros en el proceso penal”, (2004) nos. 1–3 *Revista de Derecho Procesal*, 50.
- 21 This was already stated in the benchmark case ECtHR, 25 March 1998, *Kopp v. Switzerland*, Appl. no. 13/1997/797/1000. Although, in the end, the case was analysed from the perspective of insufficient legal provision, the Court highlighted the difficulty in avoiding privileged communications from being intercepted. See also ECtHR, 3 February 2015, *Pruteanu v. Romania*, Appl. no. 30181/05; ECtHR, 16 November 2021, *Vasil Vasilev v. Bulgaria*, Appl. no. 7610/15.
- 22 On the different approach towards the exclusionary rules of evidence in this context, see L. Bachmaier and S. Thaman, “A Comparative View of the Right to Counsel and the Protection of Attorney-Client Communications” in L. Bachmaier Winter, S. Thaman, and V. Lynn, (eds.), *The Right to Counsel and the Protection of Attorney-Client Communications in criminal proceedings. A Comparative View*, 2020, pp. 101 and 104.
- 23 This is the case, for example, in Portugal, Spain, and in several states of the USA, precisely Oregon and Minnesota. See L. Bachmaier and S. Thaman, *op. cit.* (n. 22), p. 55.
- 24 This was the case in ECtHR, 25 February 2003, *Roemen and Schmit v. Luxembourg*, Appl. no. 51772/99. See also ECtHR, 4 February 2020, *Kruglov and Others v. Russia*, Appl. no. 11264/04 *et al.*, para. 128.
- 25 ECtHR, 25 July 2013, *Khodorkovskiy and Lebedev v. Russia*, Appl. nos. 11082/06, 13772/05.
- 26 See ECtHR, 19 September 2002, *Tamosius v. United Kingdom*, Appl. no. 62002/00 (inadmissibility decision in a tax fraud case). See also ECtHR, 1 December 2015, *Brito Ferrinho Bexiga Vila-Nova v. Portugal*, Appl. no. 69436/10; ECtHR, 13 January 2009, *Sorvisto v. Finland*, Appl. no. 19348/04, para. 118; ECtHR, 15 February 2011, *Heino v. Finland*, Appl. no. 56720/09, para. 43.
- 27 See, for example, ECtHR, 27 September 2005, *Petri Sallinen and Others v. Finland*, Appl. no. 50882/99. See extensively L. Bachmaier, “Lawyer-client privilege”, *op. cit.* (n. 7), 22 ff.
- 28 ECtHR, 17 December 2020, *Saber v. Norway*, Appl. no. 459/18.
- 29 See ECtHR, *Kruglov and Others v. Russia*, *op. cit.* (n. 24).
- 30 The frequent practice of cloning or mirroring the entire hard drive, both in direct computer searches and in remote computer searches, inevitably leads to the interception and seizure of documents and communications that should be excluded, because they fall under the lawyer-client privilege. See, L. Bachmaier Winter, “Remote search of computers under the new Spanish Law of 2015: proportionality principle and the protection of privacy”, (2017) 129(1) *Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW)*, 1–27.
- 31 ECtHR, 3 July 2012, *Robathin v. Austria*, Appl. no. 30457/06, paras. 47, 51, 52. See also ECtHR, 22 May 2008, *Iliya Stefanov v. Bulgaria*, Appl. no. 65755/01; ECtHR, 4 October 2018, *Leotsakos v. Greece*, Appl. no. 30958/13, paras. 43, 52; 12 February 2015, ECtHR, *Yuditskaya and Others v. Russia*, Appl. no. 5678/06.
- 32 On these safeguards, see, in more detail, L. Bachmaier Winter, “Lawyer-client privilege and computer searches in law offices: the caselaw of the European Court of Human Rights and the need for common standards in transnational criminal investigations in the EU”, in: M. Daniele and S. Signorato (eds.), *Volume in Onore Prof. Kostoris*, 2022, pp. 261–286, 267 ff.
- 33 See ECtHR, *Tamosius v. United Kingdom*, *op. cit.* (n. 26).
- 34 See, in particular: ECtHR, *Roemen and Smit v. Luxembourg*, *op. cit.* (n. 24), para. 69; ECtHR, 16 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria*, Appl. no. 74336/01; ECtHR, *André and Another v. France*, *op. cit.* (n. 15), paras. 42 and 43; ECtHR, 1 September 2009, *Jacquier v. France*, Appl. no. 45827/07; ECtHR, 21 January 2010, *Xavier Da Silveira v. France*, Appl. no. 43757/05, paras. 37 and 43; ECtHR, 3 September 2015, *Sérvulo & Associados – Sociedade de Advogados RI v. Portugal*, Appl. no. 27013/10; ECtHR, *Sommer v. Germany*, *op. cit.* (n. 13), para. 56; ECtHR, 17 May 2018, *Wolland v. Norway*, Appl. no. 39731/12, para. 75.
- 35 ECtHR, *Yuditskaya and Others v. Russia*, *op. cit.* (n. 31); also: ECtHR, *Kruglov and Others v. Russia*, *op. cit.* (n. 24), para. 132; ECtHR, *Iliya Stefanov v. Bulgaria*, *op. cit.* (n. 31), para. 43.
- 36 On the search of computers in lawyer’s offices, see ECtHR, *Petri Sallinen and Others v. Finland*, *op. cit.* (n. 27); ECtHR, *Wieser and Bicos Beteiligungen GmbH v. Austria*, *op. cit.* (n. 34).
- 37 ECtHR, *Wolland v. Norway*, *op. cit.* (n. 34).
- 38 On this judgment, see L. Bachmaier Winter (2022), “Lawyer-client privilege and computer searches in law offices...”, *op. cit.* (n. 32), pp. 275–276.
- 39 ECtHR, 16 November 2021, *Särgava v. Estonia*, Appl. no. 698/19, paras. 99 and 100.
- 40 *Ibid.* para. 102.
- 41 *Ibid.* paras. 98 and 103.
- 42 With regard to the lack of safeguards in the seizure of electronic data, see also ECtHR, 3 December 2019, *Kirdök and Others v. Turkey*, Appl. no. 14704/12, paras. 52–57.
- 43 See Guidelines on Digital Forensic Procedures for OLAF Staff, *op. cit.* (n. 6).
- 44 Article 6.3 of the Guidelines, *op. cit.* (n. 6).
- 45 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, 18.
- 46 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, 118. Although the Regulation will be applicable from 18 August 2026 onwards only, certain aspects already affect the right to lawyer-client confidentiality which should be pointed out here.
- 47 See Art. 11(1) lit. a) and Recital 20 DEIO.
- 48 See L. Bachmaier, “Mutual Admissibility of Evidence and Electronic Evidence in the EU – A New Try for European Minimum Rules in Criminal Proceedings?”, (2023) *eu crim*, 223–229.
- 49 On the need to establish general principles for transnational criminal proceedings, see J. Vervaele and S. Gless, “Law Should Govern: Aspiring General Principles for Transnational Criminal Justice”, (2013) 9(4) *Utrecht Law Rev.*, 1–10; see also, S. Gless, *Beweisgrundsätze einer grenzüberschreitenden Rechtsverfolgung*, 2007, pp. 142 ff.
- 50 I only refer to the Production Order, because the Preservation Order (although also entailing interference in data protection rights of a person by ordering the retention of such data until the Production Order is being issued) does not pose problems as to evidence transfer and admissibility.
- 51 Recital 63 EPO/EPRO-Regulation.



# Enhancing the Right of Access to a Lawyer for Detained Suspects and Accused Persons via Videoconferencing

## The Situation in Germany and Proposals for Improvement

Tomohiro Nakane

This article discusses access to a lawyer via videoconferencing for detained suspects and accused persons. In today's digital age, the introduction of videoconferencing leads to enhance the right of access to a lawyer for suspects and accused persons under Directive 2013/48/EU. The article first provides an overview of the current provisions of the Directive, then analyses the situation in Germany (which has already introduced access to a lawyer by means of videoconferencing), and lastly shows the benefits of access to a lawyer via videoconferencing. A revision of Directive 2013/48/EU in order to enshrine this right is proposed in the last section.

### I. Introduction

Criminal proceedings have become increasingly digitalised in recent years. Videoconference hearings have been provided for in many EU laws since the 2000s, in both civil and criminal cases. In 2013, the Council released a guide on the use of videoconferencing in cross-border proceedings. Since the COVID-19 pandemic, the introduction of videoconferencing in judicial proceedings has progressed even further. In 2020, the European Criminal Bar Association published guidelines on remote hearings and interviews of suspects and accused persons by means of videoconference. The Council of Europe released guidelines on videoconferencing in judicial proceedings in 2021. And Art. 5 and 6 of the 2023 Regulation on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial, and criminal matters provide for hearings via videoconference. Discussions on the introduction of videoconferencing have so far mainly focused on hearings in cross-border cases.

However, videoconferencing's pivotal role in facilitating immediate legal access for detained suspects and accused persons highlights a critical and specific area of application, especially during the crucial pre-trial phase. The digitalisation of criminal proceedings thus provides an opportunity to enhance the right of access to a lawyer for suspects and accused persons under Directive 2013/48/EU. The practice of allowing detained suspects and accused persons access to a lawyer via videoconference has become widespread in Germany in recent years (predominantly Skype is used). This is a major step forward in enhancing the right of access to a lawyer, but there are still areas that need to be

improved. To date, there is no literature in Germany directly addressing access to a lawyer via videoconferencing for detained suspects and accused persons (indirectly: see III. 4), and the issue also has not been addressed in international journals. Therefore, this article examines what future revisions of Directive 2013/48/EU are needed in the age of digitalisation – through a discussion of access to a lawyer via videoconferencing in Germany.

The article first reviews the provisions of Directive 2013/48/EU (II), then analyses the current practice in Germany of access to a lawyer for detained suspects and accused persons via videoconference in Germany (III). This is followed by a discussion on the benefits of access to a lawyer by means of videoconference and how Directive 2013/48/EU should be revised in the digital age (IV) before conclusions on the matter are drawn (V).

### II. Provisions on the Right of Access to a Lawyer in Directive 2013/48/EU

Art. 3(1) of Directive 2013/48/EU provides that suspects and accused persons have the right of access to a lawyer in such time and manner as to allow them to exercise their rights of defence in a practical and effective manner. The right of access to a lawyer entails the right to meet and communicate in private with the lawyer representing them (Art. 3(3)(a)). Suspects or accused persons have access to a lawyer at the earliest time and without undue delay after deprivation of liberty (Art. 3(2)(c)). The confidentiality of communications, including meetings, correspondence, telephone conversations, and other forms of communi-

cation permitted under national law between suspects or accused persons and their lawyer, is guaranteed (Art. 4). Confidentiality of communication between suspects or accused persons and their lawyer is key to ensuring the effective exercise of the rights of the defence and is an essential part of the right to a fair trial (Recital 33). Member States “may” make practical arrangements concerning the use of videoconferencing and other communication technologies to enable communication with a lawyer (Recital 23). It is thus left to the discretion of Member States whether or not to introduce communication by means of videoconference between suspects or accused persons and their lawyer.

In exceptional circumstances and only at the pre-trial stage, Member States may allow a delay in access to a lawyer where the geographical remoteness of a suspect or accused person makes it impossible to ensure the right of access to a lawyer without undue delay after deprivation of liberty (Art. 3(5)). In such cases, the competent authorities should not question the person concerned or carry out any of the investigative or evidence-gathering acts provided for in this Directive until access to a lawyer has been secured (Recital 30). Where immediate access to a lawyer is not possible because of the geographical remoteness of the suspect or accused person, Member States should arrange for communication via telephone or videoconference, unless this is impossible (Recital 30). The addition of the phrase “unless this is impossible” means that Member States are not obliged to introduce these means of communication if their introduction would be difficult because of technical difficulties or the risk of absconding or destroying evidence. Thus, the Directive requires Member States to introduce either videoconferencing or telephoning only on the grounds of geographical remoteness.

In the case of the European Arrest Warrant, a requested person has the right of access to a lawyer in the executing Member State without undue delay after arrest (Art. 10(1) and (2)(a)). Member States “may” make practical arrangements concerning the duration, frequency, and means of communication between requested persons and their lawyer, including concerning the use of videoconferencing and other communication technologies to facilitate such communication (Recital 44). Thus, even in the case of the European Arrest Warrant, the introduction of videoconference communication is left to the discretion of the Member States.

In Germany, the implementation of Directive 2013/48/EU did not address the introduction of access to a lawyer via videoconference.

Furthermore, neither the European Prison Rules nor the Nelson Mandela Rules provide for the right of access to a lawyer via videoconference for detained suspects and accused persons.

### III. Extended Access to a Lawyer by Means of Videoconference in Germany

#### 1. Legislative development

Art. 148(1) of the German Code of Criminal Procedure provides that suspects and accused persons have the right to communicate with their defence counsel in writing and orally, even when they are in custody. In the literature, oral communication in Art. 148(1) is understood to include telephone calls, but it is not clear whether new tools such as videoconferencing are included. Prior to the 2006 constitutional amendment, the rules governing pre-trial detention in Germany, including access to a lawyer, were governed by the Federal Rules on the Execution of Pre-Trial Detention (*Untersuchungshaftvollzugsordnung*). No. 38 of the Federal Rules allowed communication by telephone and telegram between pre-trial inmates and persons outside the penal institution. Similarly, Art. 32 of the Federal Prison Act (*Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung*) also provided for communication by telephone and telegram for convicted prisoners. In 2006, a constitutional amendment placed the execution of pre-trial detention and imprisonment under the jurisdiction of the *Länder*, the German federal states.

In 2011, the *Länder* of Berlin, Brandenburg, Bremen, Mecklenburg-Western Pomerania, Rhineland-Palatinate, Saarland, Saxony, Saxony-Anhalt, Schleswig-Holstein, and Thuringia jointly released a Model Bill for Prison Acts of the *Länder* (*Musterentwurf zum Landesstrafvollzugsgesetz*). Art. 36 (Other forms of telecommunication) of this Model Bill provides that if “other forms of telecommunication” other than the telephone are authorised by the supervisory authority, the head of the penal institution may permit prisoners to use these forms of telecommunication at their own expense. “Other forms of telecommunication” includes videoconferencing.

In addition, the *Länder* of Berlin, Brandenburg, Bremen, Hamburg, Hesse, Rhineland-Palatinate, Saarland, Saxony, Saxony-Anhalt, Schleswig-Holstein, and Thuringia jointly released a Model Bill for Acts of the *Länder* on the Execution of Pre-Trial Detention (*Musterentwurf der Untersuchungshaftvollzugsgesetze der Bundesländer*). Art. 40 of

this Model Bill provides for communication by telephone, but there is no article on other forms of telecommunication (such as videoconferencing). The exclusion of forms of telecommunication other than the telephone has been criticised as outdated.

When the *Länder* first introduced their pre-trial detention acts, only the Act of Hesse provided for other forms of telecommunication. The Acts of Brandenburg, Hamburg, Mecklenburg-Western Pomerania, Rhineland-Palatinate, and Schleswig-Holstein provided only for telephone provisions and stated in the explanatory memoranda to their respective bills that other forms of electronic telecommunication were, in principle, not permitted, because the potential for abuse and the costs of controlling such abuse were too high.

Subsequently, the Acts of Brandenburg, Hamburg, North Rhine-Westphalia, Rhineland-Palatinate, Saarland, Saxony-Anhalt, and Thuringia introduced articles on other forms of telecommunication. Additionally, in response to the COVID-19 pandemic, Schleswig-Holstein introduced relevant legislation in 2021, followed by Baden-Württemberg and Bavaria in 2022. As of 1 March 2024, 11 out of 16 acts of the *Länder* provide for other forms of telecommunication.

## 2. Videoconferencing provisions and objectives

The contents of the provisions of the articles on other forms of telecommunication in the respective acts of the *Länder* are largely the same. The statutory text of Baden-Württemberg is used here as an example. The relevant article provides for a two-step procedure. First, the supervisory authority (the federal state's Ministry of Justice) grants authorisation only if the abstract risk to the security of the penal institution can actually be controlled. As a second step, the head of the institution decides on an individual permit for use. According to the websites of several penal institutions of the *Länder*, videoconferencing at the pre-trial stage has currently been introduced in practice in at least 12 *Länder* (see table below). Several *Länder* have introduced videoconferencing, despite the absence of a provision on other forms of telecommunication. Inmates do not have an individual right to obtain or be granted authorisation for this. The costs of any other forms of telecommunication are, in principle, borne by the inmates themselves. Only in well-founded exceptional cases, when inmates are not in a position to bear the costs, is it possible for the institution to bear a reasonable part of the costs. In the case of videoconferences, which fall somewhere between telephony and visits, the rules on telephony specifically apply, and the rules on visits in so far as they regulate visual surveillance. Therefore, all videoconferences between an inmate and a

lawyer are permitted and unmonitored. Whether videoconferencing is actually introduced varies from institution to institution as does the duration, frequency, and conditions under which it is used. There are no restrictions on where lawyers can use videoconferencing in any penal institution, so lawyers are free to use it from anywhere.

The purpose of this provision in Baden-Württemberg is to take into account the progressive development of communication media on the one hand and the changes in communication and information behaviour on the other. Another reason for the provision is that, since the pre-trial inmates have not yet been sentenced, they should have access to the same means of telecommunication as members of the general public, underscoring the approach that inmates should be treated as similarly as possible to members of the general public.

Other arguments are given, for instance, by the federal state of Bavaria, which introduced videoconferencing after the COVID-19 pandemic and explained its reasons as follows: The feedback from the ministries of justice of other federal states, which already provide for more extensive telecommunication possibilities for inmates, does not reveal any serious reasons against the extension of telephone communication for inmates. Since the outbreak of the pandemic, inmates' communication has already been expanded from available budget funds, so that terminals needed at short notice have already been procured. Videoconferencing has also been made available to inmates in some Bavarian penal institutions. The Bavarian Ministry of Justice carried out a comprehensive evaluation of the experience of extending telecommunications facilities in Bavarian penal institutions during the COVID-19 pandemic, with positive results. In view of this result, the possibility of authorising other forms of telecommunication (e.g., videoconferencing) has also been regulated by law. Videoconferencing can also be an important element of psychological relief for inmates in acute crisis situations. The wording "other forms of telecommunication" is intended to open up the possibility of using forms of not yet widely used telecommunication. Thus, the objectives of introducing videoconferencing do not include strengthening the right of access to a lawyer for detained suspects and accused persons.

## 3. Videoconferencing as a tool

In Germany, Skype is used as a videoconferencing tool in most penal institutions. It is unclear why Skype is used and, for example, Zoom is not. The websites of some penal institutions state that users themselves carry the risk of their

Skype calls being monitored. As Skype is provided by the American operator Microsoft, its operation is not subject to the data protection rules that apply in Germany or other European countries. This means that all data exchanged when using Skype (sounds and images, spoken words, and the contents of conversations) are transmitted unencrypted to the USA. It is therefore possible that third parties may access this data during or after transmission. It is also possible that this data may be collected, stored, modified, read, linked, or otherwise processed by Microsoft or third parties in the United States. On the other hand, the Wittlich Penal Institution in Rhineland-Palatinate, which introduced access to a lawyer via videoconferencing in February 2024, has chosen “Sichere-Videokonferenz.de” as its videoconferencing tool. The team at Horizon44 GmbH, based in Munich, Germany, operates this application. It is more secure than other providers, as well as anonymous, and data protection complies with the technical and organisational measures in accordance with the General Data Protection Regulation (GDPR). Conversations between two participants using this application are protected by encryption. Unlike other providers, Sichere-Videokonferenz.de does not store any call content on its server, and even users cannot record videoconferences. The communication is therefore comparable to a normal face-to-face conversation without the participation of unwanted third parties. The use of such a tool can ensure the confidentiality of communications between suspects or accused persons and their lawyers.

The table on page 234 shows whether there are provisions for other forms of telecommunication for pre-trial inmates in each federal state and whether videoconferencing has actually been introduced in each federal state.

#### 4. Literature on other forms of telecommunication for pre-trial inmates

Schulze, who compared acts of the *Länder* on the execution of pre-trial detention in his dissertation, supports access of suspects and accused persons to people outside the penal institution via videoconferencing for the following reasons: As a consequence of the presumption of innocence, acts of the *Länder* on the execution of pre-trial detention should include provisions covering all communication media. In today's communication society, not only telephones but also internet telephony, especially videotelephony, have long since become the norm. The cost of introducing internet telephony for pre-trial inmates is not an issue. *Länder* that do not provide for other forms of communication overemphasise security aspects, while neglecting the fact that new control possibilities are also developing. *Länder* cannot use lack of resources as an excuse and must take “all appropri-

ate and necessary measures to avoid restricting the rights of pre-trial inmates”. Therefore, other forms of telecommunication, in particular via the internet, should be made available in pre-trial detention.

#### IV. The Need for Access to a Lawyer by Means of Videoconference and the Revision of Directive 2013/48/EU

As mentioned above, the possibility for detained suspects and accused persons to have access to a lawyer by means of videoconference have been extended in Germany in recent years. However, under German law, access to a lawyer via videoconference is not recognised as a right *per se* for suspects and accused persons and is only available if an article on other forms of telecommunication is provided for in an act of a federal state and authorised by the supervisory authority, and only in accordance with the conditions of the penal institution. Skype – the tool that is predominantly used in penal institutions in Germany – is also not suitable for unmonitored communication with a lawyer due to the lack of encryption and data protection rules. It follows that access to a lawyer by means of videoconference is not adequately provided for in Germany.

Directive 2013/48/ EU leaves it up to the Member States to introduce access to a lawyer via videoconference. However, Art. 3(1) of Directive 2013/48/EU provides that suspects and accused persons have the right of access to a lawyer “in such time and in such a manner so as to allow the persons concerned to exercise their rights of defence practically and effectively”. In addition, suspects or accused persons are to have access to a lawyer at “the earliest” time and “without undue delay” after deprivation of liberty (Art. 3(2)(c)). Videoconferencing enables suspects and accused persons to have rapid access to their lawyers. Videoconferencing is particularly useful in cases in which urgent contact with a lawyer is needed, such as first contact, when the distance between the lawyer's office and the penal institution is considerable, or when access to the penal institution is difficult for reasons beyond one's control (e.g., bad weather).

Unlike visits, videoconferencing does not require time for travel, which allows for frequent access by the defence to suspects and accused persons, thereby enhancing their right of access to a lawyer. Furthermore, in cases in which the suspect or accused person denies the offence, or in complex cases, frequent contact with the lawyer by means of videoconference allows for careful preparation of the trial and thus also enhances the right to a fair trial (Art. 14(1)

**Table: Implementation of Videoconferencing in Each Federal German State (as of 1 March 2024)**

Federal German State	Provision on other forms of telecommunication for pre-trial inmates	Introduction of videoconferencing for pre-trial inmates
Baden-Wuerttemberg	✓	✓
Bavaria	✓	✓
Berlin	–	–
Brandenburg	✓	No information about videoconferencing on the websites of the penal institutions.
Bremen	–	✓ There is no statutory basis for this, but the Bremen Penal Institution website provides information about videoconferencing with relatives, and it is not clear which tool is used.
Hamburg	✓	No information about videoconferencing on the websites of the penal institutions. The introduction of Skype is currently under consideration.
Hesse	✓ The provision limits this to cases where there are important reasons (Art. 28(1) HUVollzG).	✓
Mecklenburg-Western Pomerania	There is no statutory basis for this but, according to the explanatory memorandum to the bill, it is permitted in exceptional cases.	✓
Lower Saxony	–	✓ There is no statutory basis for this, but Skype is available in several penal institutions.
North Rhine-Westphalia	✓	✓
Rhineland-Palatinate	✓	✓
Saarland	✓	✓
Saxony	✓	✓ There is no statutory basis for this, but according to the website of the Zwickau Penal Institution, Skype calls are only permitted with relatives.
Saxony-Anhalt	✓	No information about videoconferencing on the websites of the penal institutions.
Schleswig-Holstein	✓	✓ The Lübeck Penal Institution website only provides information about videoconferencing with relatives, and it is not clear whether the tool is Skype.
Thuringia	✓	✓

ICCPR, Art. 47 CFR, and Art. 6(1) ECHR). These enhancements, in turn, contribute to a speedy trial (see Art. 14(3)(c) ICCPR, Art. 47 CFR, and Art. 6(1) ECHR). As mentioned in Section III. 2 above, a videoconference should also be introduced from the perspective of psychological relief (unlike the telephone) for pre-trial inmates and the principle of the presumption of innocence (Art. 3 Directive (EU) 2016/343), and financial considerations should not be an issue. Videoconferencing and facial recognition technology can be used together to prevent impersonation of lawyers.

In addition to these considerations, videoconferencing for suspects and accused persons is corroborated by the – albeit non-binding – international prison rules: European Prison Rule 98.2 provides that “all necessary facilities” shall be provided to assist untried prisoners in preparing their defence and meeting with their lawyers. In addition, Nelson Mandela Rules 120(1) and 61(1) provide that inmates shall be provided with “adequate opportunity, time, and facilities” to communicate and consult with a lawyer without delay. In accordance with Rule 111(2), inmates are presumed



innocent until proven guilty and shall be treated as such. The introduction of access to a lawyer via videoconference is therefore in line with European and international legal standards.

Hence, Directive 2013/48/EU should be revised to bring it into line with these European and international standards and should explicitly provide for the right of suspects and accused persons to have access to a lawyer by means of videoconference, including in the case of a European Arrest Warrant. In the modern digital age, this should no longer be left to the discretion of Member States. It should also be explicitly provided that confidentiality is also guaranteed in the case of access to a lawyer via videoconference, as there is a risk of surveillance by police officers. In doing so, the confidentiality of communications between suspects or accused persons and their lawyers should be ensured by requiring the use of tools such as “Video-Konferenz.de”, which are free from surveillance risks, instead of common tools such as Skype. Moreover, if access to a lawyer by means of videoconference is to become a right for suspects and accused persons, it should be explicitly established that it is guaranteed free of charge.

## V. Conclusion

Although the example of Germany demonstrated that access to a lawyer via videoconference has brought improvements to the right of access to a lawyer in some respects, a revision of Directive 2013/48/EU, in line with digitalisation, is essential to harmonise the enhancement of the right of access to a lawyer for suspects and accused persons in all EU Member States.

The analysis in this article also reaffirmed that the right of access to a lawyer via videoconference offers many benefits at a low cost. On the one hand, it is important for lawyers to visit penal institutions and to communicate face-to-face in order to build trust with suspects and accused persons. On the other, the telephone, unlike a videoconference, does not require a personal computer or tablet setting and can be used to communicate messages quickly. Therefore, the right of access to a lawyer for suspects and accused persons should be more effectively enhanced through a combination of all three means of communication: visits, telephone calls, and videoconferencing. Digitalisation is surely an opportunity to strengthen the rights of suspects and accused persons.

1 E.g., Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union – Council Declaration on Article 10(9) – Declaration by the United Kingdom on Article 20, OJ C 197, 12.7.2000, 3, Art. 10; Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters, OJ L 174, 27.6.2001, 1, Art. 10(4) and 17(4).


2 General Secretariat of the Council, “Guide on Videoconferencing in Cross-border Proceedings”, *European Union* <<https://op.europa.eu/en/publication-detail/-/publication/bdbbd7f4-7da8-479d-ad83-0b56463d8e32/>> accessed 1 March 2024.

3 European Criminal Bar Association, “Statement of Principles on the Use of Video-conferencing in Criminal Cases in a Post-Covid-19 World”, *European Criminal Bar Association* <<https://www.ecba.org/content/index.php/publications/statements-and-press-releases/789-ecba-statement-on-video-conferencing-in-criminal-cases>> accessed 1 March 2024.

4 European Commission for the Efficiency of Justice (CEPEJ), “Guidelines on Videoconferencing in Judicial Proceedings”, *Council of Europe* <<https://edoc.coe.int/en/efficiency-of-justice/10706-guidelines-on-videoconferencing-in-judicial-proceedings.html>> accessed 1 March 2024. See also Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, CETS No. 182, 8.11.2011, Art. 9; Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, CETS No. 224, 12.5.2022, Art. 11.

5 Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial

**Dr. Tomohiro Nakane, LL.M. (Passau)**  
Lecturer, Graduate School of Law, Nagoya University, Japan



and criminal matters, and amending certain acts in the field of judicial cooperation, OJ L, 2023/2844, 27.12.2023.

6 Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294, 6.11.2013, 1.

7 European Prison Rule 99(b) provides that untried prisoners may communicate with their family members and other persons by other forms of communication. “Other forms of communication” include electronic communication. Council of Europe, *European Prison Rules*, 2006, pp. 95, 52. There is no provision, however, for access to a lawyer via electronic communication (see Rule 98.2).

8 Nelson Mandela Rule 58(1)(a) provides for prisoners to communicate with family and friends by electronic and digital means, but electronic and digital communication with lawyers is not provided for (see Rules 120(1) and 61). United Nations General Assembly, “United Nations Standard Minimum Rules for the Treatment of

- Prisoners (the Nelson Mandela Rules)", A/RES/70/175, 8.1.2016, 1.
- 9 See e.g., M. Jahn, in: J.-P. Becker *et al.* (ed.), *Löwe-Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz Vierter Band Teilband 2 §§ 137–150*, 27th ed., 2021, Art. 148, mn. 15; G. Willnow, in: C. Barthe and J. Gericke (ed.), *Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK*, 9th ed., 2023, Art. 148, mn. 7.
- 10 Gesetz zur Änderung des Grundgesetzes (Artikel 22, 23, 33, 52, 72, 73, 74, 74a, 75, 84, 85, 87c, 91a, 91b, 93, 98, 104a, 104b, 105, 107, 109, 125a, 125b, 125c, 143c), BGBl I 2034, 28.8.2006.
- 11 N. Nestler, "Der Musterentwurf für ein Landesstrafvollzugsgesetz als Konsequenz des Phlegmas um die Europäischen Strafvollzugsgrundsätze?", (2012) *Neue Kriminalpolitik*, 87, 90.
- 12 Senatorin für Justiz und Verfassung, "Musterentwurf zum Landesstrafvollzugsgesetz vom 23. August 2011", *Freie Hansestadt Bremen*, p. 25 <<https://www.justiz.bremen.de/publikationen/gesetze-verordnungen-verwaltungsvorschriften-vereinbarungen-1871>> accessed 1 March 2024.
- 13 See *ibid.*, 104.
- 14 Landtag Mecklenburg-Vorpommern, "Gesetzentwurf der Landesregierung: Entwurf eines Gesetzes über den Vollzug der Untersuchungshaft in Mecklenburg-Vorpommern (Untersuchungshaftvollzugsgesetz Mecklenburg-Vorpommern – UVollzG M-V)", Drs. 5/2764, 7.9.2009, p. 2.
- 15 H. Pollähne, in: S. König (ed.), *Anwaltskommentar Untersuchungshaft*, Art. 40, mn. 7.
- 16 *Ibid.*
- 17 Gesetz zur Schaffung und Änderung hessischer Vollzugsgesetze, GVBl I 185, 28.6.2010: Hessisches Untersuchungshaftvollzugsgesetz.
- 18 Landtag Brandenburg, "Gesetzentwurf der Landesregierung Gesetz über den Vollzug der Untersuchungshaft im Land Brandenburg (Brandenburgisches Untersuchungshaftvollzugsgesetz – BbgUVollzG)", Drs. 4/7334, 11.3.2009, p. 104.
- 19 Bürgerschaft der freien und Hansestadt Hamburg, "Mitteilung des Senats an die Bürgerschaft: Entwurf eines Gesetzes über den Vollzug der Untersuchungshaft (Hamburgisches Untersuchungshaftvollzugsgesetz – HmbUVollzG)", Drs. 19/4451, 27.10.2009, p. 34.
- 20 Landtag Mecklenburg-Vorpommern, *op. cit.* (n. 14), p. 77: Gesetz über den Vollzug der Untersuchungshaft in Mecklenburg-Vorpommern.
- 21 Landtag Rheinland-Pfalz, "Gesetzentwurf der Landesregierung: Landesuntersuchungshaftvollzugsgesetz (LUVollzG)", Drs. 15/3292, 7.4.2009, p. 45.
- 22 Schleswig-Holsteiner Landtag, Drs. 16/2726, 9.6.2009, p. 78: Gesetz über den Vollzug der Untersuchungshaft in Schleswig-Holstein.
- 23 Gesetz über den Vollzug der Freiheitsstrafe, der Jugendstrafe und der Untersuchungshaft im Land Brandenburg (Brandenburgisches Justizvollzugsgesetz – BbgJVollzG), GVBl I/13, [Nr 14], 24.4.2013.
- 24 Gesetz über den Vollzug der Sicherungsverwahrung und zur Änderung weiterer Gesetze, HmbGVBl 211, 21.5.2013: Gesetz über den Vollzug der Untersuchungshaft.
- 25 Gesetz zur Regelung des Jugendstrafvollzuges und zur Änderung der Vollzugsgesetze in Nordrhein-Westfalen, GV NRW Nr 19 483, 7.4.2017: Gesetz zur Regelung des Vollzuges der Untersuchungshaft in Nordrhein-Westfalen.
- 26 Landesgesetz zur Weiterentwicklung von Justizvollzug, Sicherungsverwahrung und Datenschutz, GVBl 79, 8.5.2013: Landesjustizvollzugsgesetz.
- 27 Gesetz Nr. 1804 zur Neuregelung des Vollzuges der Freiheitsstrafe im Saarland, Amtsbl I Nr 11 116, 24.4.2013: Gesetz über den Vollzug der Untersuchungshaft im Saarland.
- 28 Erstes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt – Vollzug der Freiheitsstrafe, der Jugendstrafe, der Untersuchungshaft und des Strafrestes (Erstes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt – JVVollzGB I LSA), GVBl LSA 666, 18.12.2015.
- 29 Thüringer Justizvollzugsgesetzbuch (ThürJVollzGB), GVBl 13, 27.2.2014.
- 30 Gesetz über den Vollzug der Untersuchungshaft in Schleswig-Holstein (Untersuchungshaftvollzugsgesetz – UVollzG), GVBl 1170, 23.9.2021.
- 31 Gesetz zur Änderung des Justizvollzugsgesetzbuchs, GBl Nr 26 410, 26.7.2022: Gesetzbuch über den Justizvollzug in Baden-Württemberg Buch 2 Untersuchungshaftvollzug.
- 32 Gesetz zur Änderung des Bayerischen Strafvollzugsgesetzes und weiterer Rechtsvorschriften, GVBl 642, 21.10.2022: Gesetz über den Vollzug der Untersuchungshaft.
- 33 By way of exception, the provision of the Act of Hesse provides that it is limited to cases where there are important reasons (Art. 28(1) HUVollzG).
- 34 Beteiligungsportal Baden-Württemberg, "Entwurf eines Gesetzes zur Änderung des Justizvollzugsgesetzbuchs", *Beteiligungsportal Baden-Württemberg*, p. 47 <<https://beteiligungsportal.baden-wuerttemberg.de/de/mitmachen/lp-17/gesetz-zur-aenderung-des-justizvollzugsgesetzbuchs#:~:text=Mit%20dem%20Entwurf%20f%C3%BCr%20ein,der%20Vollzugsziele%20gezielt%20weiterentwickelt%20werden>> accessed 1 March 2024.
- 35 *Ibid.* See also Art. 19 JVVollzGB I.
- 36 *Ibid.*
- 37 The reasons for this are not clear, but it is assumed that Skype calls are interpreted as part of a phone call.
- 38 Beteiligungsportal Baden-Württemberg, *op. cit.* (n. 34), 47.
- 39 Beteiligungsportal Baden-Württemberg, *op. cit.* (n. 34), 47.
- 40 Beteiligungsportal Baden-Württemberg, *op. cit.* (n. 34), 48. In practice, Skype appears to be provided free of charge to pre-trial inmates in many penal institutions, according to their websites.
- 41 Beteiligungsportal Baden-Württemberg, *op. cit.* (n. 34), 48.
- 42 Art. 20(2) and 15 JVVollzGB II.
- 43 Beteiligungsportal Baden-Württemberg, *op. cit.* (n. 34), 47.
- 44 Beteiligungsportal Baden-Württemberg, *op. cit.* (n. 34), 47.
- 45 Bayerischer Landtag, "Gesetzentwurf der Staatsregierung zur Änderung des Bayerischen Strafvollzugsgesetzes und weiterer Rechtsvorschriften", Drs. 18/23106, p. 1.
- 46 *Ibid.*
- 47 *Ibid.*, 5.
- 48 *Ibid.*, 5.
- 49 *Ibid.*, 5.
- 50 *Ibid.*, 6.
- 51 *Ibid.*, 6.
- 52 The reason for this is presumably that German penal institutions introduced videoconferencing via Skype before Zoom became widespread. It was used as a model for other penal institutions to introduce videoconferencing, hence the widespread use of Skype. It is also assumed that another reason is that Skype is a video call (Zoom is a video meeting), which is in line with the general understanding that the right of access to a lawyer under Art. 148(1) of the German Code of Criminal Procedure includes telephone calls.
- 53 E.g., Justizvollzugsanstalt Vechta, "Datenschutz bei Nutzung der Skype Videotelefonie", *Niedersachsen* <[https://justizvollzugsanstalt-vechta.niedersachsen.de/startseite/besuchs\\_und\\_angehorigeninformation/skype\\_videotelefonie/](https://justizvollzugsanstalt-vechta.niedersachsen.de/startseite/besuchs_und_angehorigeninformation/skype_videotelefonie/)> accessed 1 March 2024.
- 54 *Ibid.*
- 55 *Ibid.*
- 56 *Ibid.*
- 57 *Ibid.*
- 58 Justizvollzugsanstalt Wittlich, "Besuch von Gefangenen in der Justizvollzugsanstalt Wittlich", *Rheinland-Pfalz* <<https://jvawt.justiz.rlp.de/de/service-informationen/besuchsregelung/>> accessed 1 March 2024.
- 59 Sichere-Videokonferenz.de, "Hilfe & FAQ", *Sichere-Videokonferenz*.

de <<https://sichere-videokonferenz.de/faq/>> accessed 1 March 2024.

60 *Ibid.* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, 1.

61 *Ibid.*

62 *Ibid.*

63 *Ibid.*

64 Justizvollzugsanstalt Bremen, "Besucherinformationen", *Freie Hansestadt Bremen* <<https://www.jva.bremen.de/besucher-info-1471>> accessed 1 March 2024.

65 Bürgerschaft der freien und Hansestadt Hamburg, "Schriftliche Kleine Anfrage der Abgeordneten Cansu Özdemir (DIE LINKE) vom 26.08.20 und Antwort des Senats", Drs. 22/1195, 1.9.2020, p. 6.

66 Landtag Mecklenburg-Vorpommern, *op. cit.* (n. 14), 77.

67 E.g., Justizvollzugsanstalt Vechta, *op. cit.* (n. 53).

68 Justizvollzugsanstalt Zwickau, "Besuch/Skype", *Sachsen.de* <<https://www.justiz.sachsen.de/jvaz/besuch-4096.html>> accessed 1 March 2024.

69 Justizvollzugsanstalt Lübeck, "Informationen zum Kontakt mit männlichen Gefangenen", *Schleswig-Holstein* <[https://www.schleswig-holstein.de/DE/justiz/gerichte-und-justizbehoerden/JVALUEBECK/Gefangene/\\_documents/maennliche\\_gefangene.html](https://www.schleswig-holstein.de/DE/justiz/gerichte-und-justizbehoerden/JVALUEBECK/Gefangene/_documents/maennliche_gefangene.html)> accessed 1 March 2024.

70 Jan Peter Schulze, *Die Untersuchungshaftvollzugsgesetze der Länder im Vergleich*, 2017, p. 247.

71 *Ibid.*, 248.

72 *Ibid.*, 248.

73 *Ibid.*, 248.

74 *Ibid.*, 248; Bundesverfassungsgericht (BverfG) [German Federal Constitutional Court], (2008) *Neue Zeitschrift für Strafrecht* (NStZ), 521, 522.

75 *Ibid.*, 247.

# Transnational Virtual Criminal Trials in the European Union

## Reflections on Occasion of Joined Cases C-255/23 (AVVA and Others) and C-285/23 (Linte) at the CJEU

Judit Szabó and Dominik Brodowski

In the wake of the COVID-19 pandemic, the convening of "virtual" and "hybrid" meetings through videoconferencing technology has become a common practice. This trend has also reached the sphere of criminal justice, as more and more jurisdictions, such as Hungary, are authorising hearings and trials to be held without the physical presence of all persons involved. At the same time, yet other criminal justice systems, such as that in Germany, are highly sceptical about any weakening of the requirement that the accused be physically present in the courtroom.

Recently, a Latvian court requested guidance from the CJEU as to whether criminal trials employing videoconferencing technology may be held across intra-EU borders, in particular when use of the European Investigation Order (EIO) is made. On procedural grounds, the CJEU, in its judgement of 6 June 2024, refrained from deciding issues relating to the interpretation of Directive 2014/41/EU in different but authentic languages as well as whether the accused not only has a right but also a duty to be present at trial.

In our contribution, we approach the topic of transnational virtual criminal trials in the EU through the examples of the Hungarian and the German criminal justice systems and through the two cases put before the CJEU. We will focus on the main trial, excluding other phases of the criminal procedure, such as hearings and questioning of the accused or of witnesses in the pre-trial investigation. We will also elaborate on principles of criminal justice as well as on the availability of the EIO when conducting virtual trials. Lastly, a discussion will follow with an outlook on future legislative options.

### I. The Emergence of Virtual Criminal Trials

Technological developments in the last few decades, such as the emergence of electronic communication, have undoubtedly raised challenges for the criminal justice system.

However, they have also opened up opportunities to transform communication between authorities and the persons involved in the proceedings. This digital transformation of the criminal process facilitates the exercise of procedural rights,<sup>1</sup> and its benefits include increased cost-effectiveness,

sustainability, the speeding up of procedures, and – by avoiding physical interaction – improved witness protection.<sup>2</sup>

As will be elaborated in more detail below (II.1.), the right to a fair trial is a fundamental principle of a democratic society, and the right of suspects or accused persons to be present at trial is based on this right and must be guaranteed throughout the European Union. Consequently, one of the specific features of trials *in absentia* is that an element of the right of the defence and an element of the right to a fair trial is missing: the possibility for the accused to exercise their rights whilst physically present. Moreover, the principles of immediacy and oral presentation of evidence, and potentially also the search for the “substantive” truth, may be achieved more effectively if the accused is (physically?) present at the trial. However, the emergence of virtual criminal trials has complicated the situation and warrants a detailed analysis.

### 1. Expansion of virtual criminal trials – the example of Hungary

In Hungary, the Criminal Procedure Act (CCP)<sup>3</sup>, which has been in force since 1 July 2018, represents a break with the country’s previous approach: the presence of the accused at the (main) trial is no longer an obligation, but a right of the accused. Accordingly, the accused may decide to waive their right to attend the trial (§ 430 CCP). Moreover, an accused may also decide to attend the trial via a closed telecommunications network, e.g., when they are abroad (§ 121 CCP). The court, the prosecution service, or the investigating authority may order the use of a telecommunications device *ex officio* or in response to a motion filed by the person obliged or authorised to attend the procedural act (§ 121(1) CCP). The use of a telecommunications device is mandatory in cases where a procedural act requires the attendance of an aggrieved party needing special protection, or where a witness or defendant who is detained is under personal protection or in a protection programme (§ 122(1) CCP). Additionally, a recent amendment allows for the virtual attendance of other actors in the criminal proceedings, extending beyond witnesses and experts to include the defence and the prosecutor (§§ 126/C-D CCP) (so-called simplified telecommunication attendance).<sup>4</sup>

The rationale behind the use of simplified telecommunication attendance is that, since the communication takes place through the personal device of the person being heard, the procedural act can be conducted in a separate place where only the person being heard is present, without the involvement of any other authorities, even if the person concerned is currently in a different Member State. This legal instrument was created as a matter of necessity

by the exceptional legislation in force during the COVID-19 pandemic. Subsequently, it has become a widely adopted practice and was specifically introduced into the CCP in response to positive feedback from legal practitioners. However, due to the lower credibility of these channels, the legislation only authorises the use of devices capable of simultaneous transmission of video and audio recordings, with appropriate guarantees, such as explicit consent and active cooperation (§§ 126/A-B CCP).

### 2. Reservations against virtual criminal trials – the example of Germany

By contrast, German criminal procedures generally, as set forth in §§ 145(1), 226(1), 230(1), 338 No 5 of the German Code of Criminal Procedure (*Strafprozessordnung – StPO*)<sup>5</sup>, require the physical presence of all necessary participants (that is, the court, the public prosecutor, the defendant and, in cases of mandatory defence, their counsel)<sup>6</sup> for the main trial in criminal matters. In exceptional circumstances and in cases of minor importance, the requirement for the defendant to be present may be waived (§§ 233(1), 329(2) StPO). Furthermore, in proceedings involving several defendants, the judge may grant leave of absence to individual defendants and their counsel for parts of the trial “unless these parts of the hearing concern them” (§ 231c StPO). Yet these provisions do not allow for virtual presence to replace physical presence. The only exception is that witnesses may be interviewed and interpreters may work from a different place with a bidirectional audiovisual connection (§ 247a StPO, § 185(1a) GVG<sup>7</sup>).

While trials in civil matters may be conducted online since 2013 (§ 128a of the Code of Civil Procedure (*Zivilprozessordnung – ZPO*)), and court hearings in the execution of a sentence since 2021 (§ 463e StPO), there are considerable reservations against virtual criminal trials in Germany.<sup>8</sup> Further evidence of this scepticism can be found in the current discussions surrounding recent legislation which enables courts dealing with appeals to hold hearings by videoconference (§ 350(3) StPO<sup>9</sup>). Several political actors have expressed opposition to this provision,<sup>10</sup> while others have indicated that such a “virtualisation” must not spread to the main trial in criminal matters.<sup>11</sup>

### 3. Emerging transnational tensions – the background on CJEU Joined Cases C-255/23 and C-285/23

In view of such differing approaches, the Latvian Economic Court (*Ekonomisko lietu tiesa*) has raised the issue of virtual criminal trials to the CJEU. In the Joined Cases C-255/23 (*AVVA and Others*) and C-285/23 (*Linte*), the defendants,



who are nationals of different EU Member States (Lithuania and Germany), currently reside in their respective home countries and wish to participate in the main trial remotely by videoconference. In particular, for the German defendant in the *Linte* case (C-285/23), the requirement to be physically present poses a significant burden:

[He] is a 71-year-old pensioner who does not have sufficient income to pay his travel costs and who, with his wife, cares for his 92-year-old mother-in-law, who lives with them and needs care as a person with disability. [He] has never lived in Latvia and does not speak Latvian. Under those circumstances, it is unreasonable to expect him to move to Latvia in order to be present throughout the proceedings. [He] nevertheless wishes to participate in the trial by videoconference from Germany.<sup>12</sup>

However, the Latvian Supreme Court (*Senāts*) indicated that the Latvian Criminal Procedural Code, and in particular its provision allowing for the performance of “procedural acts using technical means (teleconference, videoconference) if the interests of the criminal proceedings so require” (Section 140(1) CCP) is limited in scope to the territory of Latvia<sup>13</sup> and cannot be applied transnationally, as this would interfere with the sovereignty of another country. Therefore, a transnational participation in a criminal trial requires “recourse to an instrument of judicial cooperation.”<sup>14</sup> Against this background, the Latvian Economic Court asked the CJEU whether Directive 2014/41/EU regarding the European Investigation Order (EIO) in criminal matters<sup>15</sup> is such an instrument allowing for transnational virtual criminal trials.

In *AVVA and Others* (C-255/23), the court asked whether Directive 2014/41/EU provides a sufficient framework, even without the issuance of an EIO and with the consent of the defendant, as long as the court is “able, by technical means, to verify the identity of the person in the other Member State and provided that person’s rights of the defence and assistance by an interpreter are ensured.”<sup>16</sup> In *Linte* (C-285/23), the court also wanted to know whether the right to be present at trial as set out in Art. 8(1) Directive (EU) 2016/343 is also met in the case of a videoconference. Otherwise, Germany would have a strong argument to refuse the execution of an EIO on the basis of Art. 11(1)(f) Directive 2014/41/EU, as this would be incompatible with the fair trial guarantee enshrined in Arts. 47 and 48 CFR.

As the Latvian court did not stay the proceedings in either case but continued to hear evidence, the CJEU responded in its judgment of 6 June 2024 that

[s]uch procedural steps [...] are liable to render the questions referred for a preliminary ruling [...] devoid of purpose and of relevance to the main proceedings, and are therefore liable to prevent the referring court from complying, in the context of the main proceedings in both cases, with the decisions by which the Court would reply to the references for a preliminary ruling.<sup>17</sup>

It was the CJEU’s worry that “the effectiveness of the cooperation mechanism provided for in Art. 267 TFEU” could be undermined and that its answers might come too late and would then be “purely advisory.” On this basis, it ruled that “there is no need to rule on the questions referred for a preliminary ruling.”<sup>18</sup> As the CJEU did not even give any indication on the substance of the questions referred to it, the underlying and emerging transnational tensions remain, and warrant further analysis.

## II. The Fundamental Question: a Right to Be Present – or a Duty to Be Present?

### 1. The right to be present at trial

The right of the accused to be present in person at trial is part of the right to a fair trial as provided for in Art. 6 European Convention on Human Rights (ECHR). However, the European Court of Human Rights (ECtHR) has consistently held that this right is not absolute. In certain circumstances, the accused may, of their own free will, expressly or implicitly but unequivocally, waive that right. As regards the use of videoconferencing technology in legal proceedings, the ECtHR has determined that this form of participation in proceedings is not in itself incompatible with the concept of a fair and public trial.<sup>19</sup> However, online hearings are subject to the fundamental requirement that they must be used only in justified cases and must always be aimed at achieving a legitimate aim. Furthermore, for a defendant to be participating in a trial online, it must be guaranteed that they can effectively participate in the trial through the chosen means of communication and that any limitation of rights caused by the online presence must be compensated by the court through other means. Effective participation by online means includes access to the technical means, uninterrupted visibility, audibility of the proceedings on both sides, and continuous participation without technical obstacles. In addition, in the ECtHR’s jurisprudence, it is of paramount importance to ensure effective and confidential communication between the accused and the defence during the online trial.<sup>20</sup>

As far as the European Union is concerned, Art. 8(1) Directive (EU) 2016/343 of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings also states that defendants have the right to be present at their trial. The Council Framework Decision 2009/299/JHA of 26 February 2009 enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person



concerned at the trial also states that attendance is a right, rather than an obligation. Therefore, the recognition and execution of a decision rendered following a trial at which the person concerned did not appear in person should not be refused, provided that the person concerned was aware of the scheduled trial and was defended at the trial by a legal counsellor mandated by them.<sup>21</sup>

Moreover, neither the above-mentioned Directive (EU) 2016/343 nor the Framework Decision 2009/299/JHA concerns the way the trial is conducted. They do not provide that a “trial” is to be understood to mean only the physical presence in person, excluding any forms of virtual attendance.

In light of the above, it remains uncertain how EU law aligns with the Hungarian simplified telecommunication attendance and similar approaches, whereby a Member State unilaterally provides online access to persons participating in proceedings without the involvement of another Member State. Furthermore, it could be argued that this raises the issue of sovereignty: does the concept of simplified telecommunication attendance require the involvement (at least by notification) of the state from which a person connects remotely to the trial – at least if this person is neither a citizen nor a resident of the state conducting the trial?

## 2. A duty to be present at the trial?

As illustrated above, the German criminal justice system pays extraordinary attention to the presence of the accused at the main trial. In the event of a defendant’s absence without leave, they will be brought before the court by force or sought for by means of an arrest warrant (§ 230(2) StPO), potentially also by a European Arrest Warrant. Likewise, in Hungary, if the accused does not confirm their attendance at the trial, the court considers them to not have waived it, and if they fail to appear when duly summoned, it may enforce their presence by means of a summons or warrant (§§ 432–433 CCP).

But is this encroachment on the liberty of a defendant who is forced to be present in the courtroom actually justified?

### a) Unfounded arguments in favour of physical presence

The guarantees of criminal procedure enshrined in Art. 6 ECHR and in Arts. 47, 48(2) CFR are not affected by a trial where the court and the prosecution are present in the courtroom and only the defendant (and potentially their counsel) joins by videoconference; hence, a duty to be present cannot be based on these factors. In particular, the trial

may remain a public hearing.<sup>22</sup> Defendants can be heard by the court on all matters of relevance; they can examine witnesses; and they are also able to intervene in discussions on matters of fact and of law remotely, at least if the technical equipment is of sufficient quality.<sup>23</sup>

The truth-finding mission of courts, which is – for instance – deeply embedded in the German criminal justice system, is also not impeded, in particular if the defendant joining the trial remotely makes use of their right to remain silent, as established in Art. 7 Directive (EU) 2016/343. Furthermore, involuntary nonverbal cues – such as sweating or blushing of a defendant – must not be taken into account by the court as evidence.<sup>24</sup> It is therefore highly problematic that the German Federal Constitutional Court has repeatedly referred to the “impression” the defendant makes upon the court as the reason for justifying their duty to be present.<sup>25</sup> However, if the defendant makes verbal statements, these can be transmitted sufficiently well by videoconferencing technology, as can voluntary nonverbal cues such as nodding.<sup>26</sup> It is also accepted practice for witnesses to be heard by videoconference.

Moreover, a duty to be present cannot be justified by referring to the purposes of subsequent punishment or by arguing that the defendants – or the public – should “feel” justice being done.<sup>27</sup> This would imply, from the outset of the trial, that defendants are in fact guilty and that they should therefore feel the pressure of criminal justice. Yet such an argument evidently contradicts their fundamental right to “be presumed innocent until proved guilty according to law” (Art. 48 (1) CFR).<sup>28</sup>

### b) Upholding the rights of the defendant

Nevertheless, the physical presence of the defendant in the courtroom will oftentimes be in their best interest. In settings where some persons are present in a room while others are connected via videoconferencing technology, the latter group will often be at a disadvantage in terms of being heard and in conveying their “message” effectively.<sup>29</sup> Moreover, those participating via videoconferencing technology might become too easily distracted; they might miss subtle cues and chances to intervene to their advantage, and be unaware of the gravity of the situation. In their absence, the trial, the judgement, and the sentencing risk may lose their human dimension and fail to adequately address the impact on the defendant.

In view of the objective to ensure fair trials (cf. Art. 6 ECHR, Art. 47 CFR), criminal justice systems must not ignore these risks associated with the physical absence of a defendant. Instead, they must, at a minimum, encourage defendants to make use

of their right to be physically present at a criminal trial. Forcing them to be physically present is surely paternalistic, but may in fact be justified by the structural deficit of autonomy of accused persons.<sup>30</sup> It is far from unheard of that defendants are not fully aware of the severity of the situation they are in. In the context of the trial, they are faced with the state making use of the strongest sword in its arsenal: criminal justice. Therefore, it is rational for them to seize any lawful chance they have to influence the trial to their advantage – and that oftentimes includes, as set out above, being physically present in the courtroom. Not doing so is presumably based on economic needs, convenience, or ignorance, but not on a rational choice. As their physical presence in the courtroom tends to be strongly to their advantage, and defendants tend to lack autonomy to make a reasonable decision on this question, the state may generally require them to be physically present in court – even contrary to their (superficial) intentions.

However, there are circumstances in which this assumption does not hold. For instance, a defendant, well represented by counsel, may make a reasonable decision to waive their right to be (physically) present in court for less important parts of the proceeding, and opt for a participation by videoconference instead. The *Linte* case (C-285/23) described above (1.3. supra) may constitute a prime example of a situation where the particular burden of physical presence tilts the balance in favour of a mere virtual presence of the accused.

### III. Using – or Mis-using? – the European Investigation Order for Transnational Virtual Criminal Trials

Considering that Latvia's legislative choice to allow for virtual criminal trials may, at least under some circumstances, be to the advantage of the defendant's situation, we now turn to the question whether this option is also available transnationally within the European Union.

#### 1. Scope of the European Investigation Order

Within the Area of Freedom, Security and Justice of the EU, the European Investigation Order, created by Directive 2014/41/EU, is a cornerstone of the implementation of the principle of mutual recognition of judicial decisions. Yet it is doubtful whether a decision by a court – such as the Latvian Economic Court – to allow a defendant to join the trial using videoconferencing technology falls within the scope of Directive 2014/41/EU.

According to Art. 1 Directive 2014/41/EU, an EIO is intended to “have one or several specific investigative

measure(s) carried out in another Member State [...] to obtain evidence”, or to “obtain[...] evidence that is already in the possession of the competent authorities of the executing State.” Art. 3 Directive 2014/41/EU further clarifies that an EIO may “cover any investigative measure with the exception of the setting up of a joint investigation team and the gathering of evidence within such a team.” It also follows from Art. 2(c)(i) and Art. 4 of the Directive that an EIO is not limited to the investigation or pre-trial phase but may also be issued by the trial court during an ongoing trial.

According to its name – European Investigation Order –, and by limiting its use to “one or several specific investigative measure(s),” the general scope of the EIO is to obtain evidence in furtherance of the investigation or prosecution. Recitals 7 and 8 of the Directive clarify that EIOs are measures “aimed at gathering evidence.” Nevertheless, questioning the defendant and giving defendants the opportunity to comment on the case at hand is only a limited part of their right to participation in the trial. The main rationale for their participation is securing their right to be heard and their right to defend themselves in the trial. Using an EIO to provide for the presence of a defendant during the trial beyond their questioning therefore seems to be outside of the scope of the EIO. This would, in turn, require recourse to different tools of judicial cooperation for transnational virtual trials.

#### 2. “Hearing by videoconference” (Art. 24 Directive 2014/41/EU)

However, taking a closer look at Art. 24(1) subpara 2 Directive 2014/41/EU, the provision could be used to argue for an extension of the scope of an EIO, as it states that an EIO may be issued “for the purpose of hearing a suspected or accused person by videoconference.”

##### a) “Hearing” in a narrower sense (as an investigative measure)

On the one hand, the term “hearing” may be construed narrowly and refer solely to the questioning of suspects and accused persons, including defendants. Such an interpretation is in line with the – equally authoritative – German language version of the Directive, which uses the term *Vernehmung*, which is best translated as “interrogation”. This interpretation would also be consistent with the general scope of the Directive and its chapter IV, which outlines “specific provisions for certain investigative measures” and is coherent with subparagraph 1, which regulates the hearing of witnesses or experts.

## b) “Hearing” in a broader sense

On the other hand, the term “hearing” is ambiguous and can be understood in a number of ways, especially from a Hungarian perspective. It can signify a hearing (*meghallgatás*), an interrogation (*kihallgatás*), or even the trial (*tárgyalás*) itself. To further complicate the situation, while the English version consistently uses “hearing” (and “hear”) throughout Art. 24 of the Directive, the Hungarian language version of the Directive, which is equally considered authoritative, uses the term *meghallgatás* in the title of Art. 24, but *kihallgatás* in paragraph 1, subpara 2. The latter term commonly refers to the procedural act of taking the statement of a witness, a suspect, or an accused person, initiated by a court or authority, at both the investigative and the judicial stages. We note – analysing Art. 24 as a whole – that the terminology is confusing and not further explained in the Directive, but in general the Hungarian jurisprudence is consistent in the separation of the aforementioned terms.

It should further be stressed that the Hungarian implementation does not limit the issuing or execution of a request for a videoconference to the investigative stage.<sup>31</sup> Rather, it interprets the opportunities offered by Art. 24 broadly, and includes, in light of the legislation cited above, the presence of the accused by videoconference at the (main) trial at which a verdict may be given.

At the same time, there is a divergence between the scope of application of the Hungarian legislation and the Directive. The Hungarian legislation lists<sup>32</sup> the witness, the accused, and the expert side by side as persons which may be heard based on Art. 24 Directive 2014/41/EU. By contrast, Art. 24(1) Directive 2014/41/EU mentions this possibility in connection with the testimony of witnesses or experts, but only makes a passing reference to the possibility of an EIO being issued in the case of a suspect or accused person. It is not evident from the Directive’s wording whether this distinction extends beyond the reference to Art. 24(5) to (7) of the Directive. Presumably, this distinction derives from the previous rule in force, Art. 10(9) of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.<sup>33</sup> It allowed for the interrogation of an accused by videoconference only where it was deemed appropriate according to the Member States’ discretion and with the consent of their competent judicial authorities; notably, this did not pose an issue in practice.<sup>34</sup>

Based on such a broad understanding of the term “hearing,” the Hungarian approach is that the spirit of the EU and the cross-border accessibility of judicial matters should allow

persons who wish to join the proceedings voluntarily from the territory of another Member State to do so. Based on this view, Art. 24 should not be interpreted restrictively, and should not exclude the possibility for Member States to unilaterally allow for virtual participation in criminal proceedings, even from the territory of another Member State and without the involvement of that other Member State.

## c) Safeguards

In addition to the general rules<sup>35</sup>, the execution of a European Investigation Order may be refused in the case of a request for a virtual hearing if the suspect or accused has not consented or if the carrying out of the investigative measure would be contrary to the fundamental principles of the law of the executing State.<sup>36</sup> The person concerned may give their consent to be questioned via telecommunications in writing, orally before a court or the prosecutor’s office, or on the record.<sup>37</sup> In addition, according to the Directive, the suspect must be informed of all their rights and duties, and an interpreter must be provided if required.<sup>38</sup> We note that the Directive is vague on the right to interpretation, as it only refers to the need to apply<sup>39</sup> the Interpretation Directive.<sup>40</sup> As a further safeguard, Hungary requires that an EIO issued by a prosecutor for the interrogation by a closed telecommunications network during the investigation requires validation by the court.<sup>41</sup>

Moreover, for all variations of “online presence”, it is necessary that the use of telecommunications equipment not negatively affect the exercise of the rights of persons participating in criminal proceedings, including the right to ask questions, to make comments and to make submissions. It must be ensured that persons present in court can see and hear those connected remotely, and that those connecting remotely are able to follow the proceedings in a meaningful way. Last but not least, if the accused is not present in the same place as their defence counsel, the direct and secure consultation between them must be made possible. According to Hungarian law, an electronic link with voice communication suffices in this regard (§ 124 CCP).

One conflict between the EIO and the Hungarian concept of simplified telecommunication attendance is, however, that the Directive, which is based on the principles of mutual recognition and loyal cooperation<sup>42</sup>, requires the transfer of an EIO and therefore a consultation (and consent) of the other affected Member State. Involving another Member State also assists in verifying the identity of the remotely connecting person, and in assuring that no unauthorised person is present at the remote location. Hungarian law states that, in case of doubt, the court may immediately interrupt the procedural act (§ 126/B para 3 CCP).

### 3. The alternative suggestion in *AVVA and Others* and *Linte*: transnational virtual criminal trials without an EIO

Considering these difficulties aligning transnational virtual criminal trials with an EIO, it is not surprising that the Latvian Economic Court also raised questions regarding alternatives to issuing an EIO. However, the court's stance in *AVVA and Others* on how Directive 2014/41/EU may permit self-executing transnational procedural acts and justify the interference with the sovereignty of the other Member States affected remains unclear, as its clear focus is regulating the issuance of EIOs. The sole exception – Art. 31 on cross-border interception of telecommunications without the assistance of the affected Member State – also requires the notification of the other Member State, and empowers it to demand the termination of the measure.

A more promising aspect is its call in *Linte* that “the use of videoconferencing in criminal proceedings with a cross-border dimension enables EU citizens to effectively exercise their freedom of movement,” and that Union law should therefore provide for such an opportunity.<sup>43</sup> However, it is still quite creative, and possibly too creative to state that the European right to be present at trial, Art. 8(1) Directive (EU) 2016/343, “includes the right of accused persons to participate effectively in the trial in a criminal case in a different Member State by videoconference from the Member State of residence.”<sup>44</sup> It is certainly true though that such an interpretation “would fit well with the prevailing emphasis on facilitating and accelerating court proceedings.”<sup>45</sup> However, the legal basis of the Directive – Art. 82(2)(b) TFEU –, its subject matter (“minimum rules concerning [...] the right to be present at the trial in criminal proceedings”, Art. 1 lit. b Directive (EU) 2016/343) and the concise wording of Art. 8(1) Directive (EU) 2016/343 (“Member States shall ensure that suspects and accused persons have the right to be present at their trial”) all argue that the European legislature has not empowered Member States in this Directive – and without any safeguards – to conduct transnational virtual criminal trials, notably without any involvement of the Member States where the defendant is physically present.

In a similar vein, Advocate General *Medina* proposed on 18 April 2024 that Art. 8(1) Directive (EU) 2016/343 does not govern the use of videoconferencing in criminal proceedings; rather, this is a matter for Member States to decide. In particular, that provision does not regulate a situation in which a criminal court gives an accused person, who is obliged to be present at the trial according to national law, the possibility to participate by videoconference in the proceedings, despite the absence of an explicit provision in national law allowing for such a mode of participation.<sup>46</sup>

In her opinion, the limited scope of the harmonisation carried out by Directive 2016/343, and the fact that it does not regulate the question whether Member States may require the defendant to be present at the trial, leads to the conclusion that the issue of mandatory presence is a matter for national law alone. This line of reasoning can be applied by analogy to the question whether Member States may provide that the right to be present at the trial can be exercised by videoconference at the request of the defendant. Since the Directive does not specify the manner in which this right is to be exercised, it leaves some leeway to Member States when it comes to specifying the means of ensuring that this right is guaranteed in their judicial systems. This allows them to provide for additional means to secure presence at the trial, such as by videoconference or by other distance communication technology, at the express request of the accused person, as long as the right to a fair trial is upheld.<sup>47</sup>

### IV. A Matter Better Decided by European Legislature

Based on our analysis, and despite the fact that the terms used in the different language versions of Art. 24 Directive 2014/41/EU are ambiguous, we are sceptical that transnational virtual criminal trials are within the scope of the EIO. In particular, authorising a “remote simplified telecommunication attendance” without even notifying the Member State the attendee is located in would bend the wording of the Directive and its foundation in the principle of mutual recognition. In a similar vein, interpreting Art. 8(1) Directive (EU) 2016/343 to include a right to a participation by videoconference, as suggested by the referring court in *Linte*, seems rather far-fetched. Despite the CJEU's reputation for advancing European integration even on subtle legal bases, it did not move forward here with expanding extra-territorial effects of criminal justice systems within the integrated European criminal justice systems.

Our analysis has shown that there are indeed situations in which the virtual presence of the accused – or of another party to the criminal proceedings – promotes the purposes of criminal justice and is of benefit to the persons involved, and where a transnational virtual criminal trial may also be more sustainable. In our view, this question should be addressed by the European legislature instead. The freshly started legislative term can provide an opportunity to discuss the appropriate legal framework, such as by amending Regulation (EU) 2023/2844,<sup>48</sup> which, in relation to criminal matters, is currently limited to specific hearings in matters concerning extradition and mutual legal assistance. In particular, this future framework could build upon Art. 8 Regulation (EU) 2023/1543<sup>49</sup> and differentiate



between the need to notify – and/or the need for consent of – the Member State which the remotely connecting person is located in. For instance, a case could be made that there is no need for such notification if the person is a citizen or resident of the Member State conducting the trial. In any case, this legal framework needs to include clear and specific safeguards for conducting transnational virtual criminal trials in full conformity with the rule of law and human rights. In particular, such safeguards would need to be far more detailed than what is prescribed in Art. 24 Directive 2014/41/EU, and would need to make sure that no one who wants to enforce their right to *physical* presence is pressured to waive this right in favour of a mere *virtual* presence.



### Dr. Judit Szabó, PhD., LL.M.

Senior lecturer, ELTE Eötvös Loránd University, Budapest, Hungary, Faculty of Law, Criminal Law Department; criminal judge, Head of the Criminal Chamber of the Budapest-Capital Regional Court



### Prof. Dr. Dominik Brodowski, LL.M. (UPenn)

Professor for Europeanization, Internationalization and Digital Transformation of Criminal Law and Criminal Procedure, Saarland University, Saarbrücken, Germany

1 See, in particular, E. Róth, “A digitalizáció és a terhelt jogok érvényesülése a büntetőeljárásban – Digitalisation and the enforcement of accused’s rights in criminal proceedings”, (2021) 2 *Miskolci Jogi Szemle*, 269.

2 A. Madarasi, “A tisztességes online tárgyaláshoz való jog – The right to a fair online trial” (2022) *Jogi Tanulmányok* <[https://epa.oszk.hu/02600/02687/00010/pdf/EPA02687\\_jogi\\_tanulmanyok\\_2022\\_427-440.pdf](https://epa.oszk.hu/02600/02687/00010/pdf/EPA02687_jogi_tanulmanyok_2022_427-440.pdf)>, 427, 428. All hyperlinks used in this article were last accessed on 7 December 2024.

3 Act XC of 2017 on the Code of Criminal Procedure (hereinafter CCP). An official translation is available at <<https://njt.hu/jogszabaly/en/2017-90-00-00>>.

4 The court in this case also sits in the courtroom equipped with a closed telecommunication system and controls the technical conduct of the hearing, while the other participants can hear and see what is happening in the courtroom and at other endpoints by clicking on a link sent to them via an online interface (without installing an application), in order to take advantage of the new communication habits associated with digitalisation and thus speed up proceedings.

5 An unofficial translation of the German Code of Criminal Procedure in English is available at <[https://www.gesetze-im-internet.de/englisch\\_stpo/index.html](https://www.gesetze-im-internet.de/englisch_stpo/index.html)>.

6 See O. Arnoldi, in: Ch. Knauer/H. Kudlich/H. Schneider (eds.), *Münchener Kommentar zur StPO*, 2nd ed., 2024, § 230, mn. 6, 10 f.; M. Deiters, in: J. Wolter/M. Deiters (eds.), *SK-StPO. Systematischer Kommentar zur Strafprozessordnung. Mit GVG und EMRK*, 6th ed., 2024, § 226 mn. 4; M. Jahn, in: J.-P. Becker et al. (eds.), *Löwe-Rosenberg. Die Strafprozeßordnung und das Gerichtsverfassungsgesetz*, 27th ed., 2021, § 145 mn. 13; B. Schmitt, in: L. Meyer-Goßner/B. Schmitt (eds.), *Strafprozessordnung mit GVG und Nebengesetzen*, 66th ed., 2023, § 230 mn. 14; L. Sommerer, “Virtuelle Unmittelbarkeit? Videokonferenzen im Strafverfahren während und jenseits einer epidemischen Lage von nationaler Tragweite”, (2021) *Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW)*, 403, 406.

7 German Courts Constitution Act (*Gerichtsverfassungsgesetz – GVG*). An unofficial translation is available at <[https://www.gesetze-im-internet.de/englisch\\_gvg/index.html](https://www.gesetze-im-internet.de/englisch_gvg/index.html)>.

8 See, in particular, M. Meißner, “Corona und Strafprozess – Zum Einsatz von Videotechnik im Strafverfahren”, *beck-blog* <<https://community.beck.de/2020/05/10/corona-und-strafprozess-zum-einsatz-von-videotechnik-im-strafverfahren>>; L. Sommerer, *op. cit.* (n. 6), 403, 445 f.; German Federal Bar (Bundesrechtsanwaltskammer, BRAK), Opinion (Stellungnahme) No. 8/2022, p. 14; and, in contrast, D. Brodowski, “Virtualisierung der strafprozessualen Hauptverhandlung”, in: B. Brunhöber et al. (eds.), *Strafrecht als Risiko. Festschrift für Cornelius Prittowitz zum 70. Geburtstag*, 2023, p. 425, 436 ff.

9 Law for a further digital transformation of the judiciary (Gesetz zur weiteren Digitalisierung der Justiz), BGBl. I 2024, Nr. 234.

10 See, for instance, German Judges’ Association (Deutscher Richterbund), Opinion (Stellungnahme) No. 28/23, p. 10; German Bar Association (Deutscher Anwaltverein), Opinion (Stellungnahme) No. 78/2023, p. 6 ff.

11 German Federal Bar (Bundesrechtsanwaltskammer, BRAK), Opinion (Stellungnahme) No. 65/2023, p. 10.

12 Latvian Economic Court (*Ekonomisko lietu tiesa*), 3 May 2023, request for a preliminary ruling in case C-285/23, unofficial English translation available at <<https://curia.europa.eu/juris/liste.jsf?num=C-285/23>>, mn. 4.

13 Latvian Economic Court, 3 May 2023, *op. cit.* (n. 12), mn. 7.

14 Latvian Economic Court (*Ekonomisko lietu tiesa*), 19 April 2023, request for a preliminary ruling in case C-255/23, unofficial English translation available at <<https://curia.europa.eu/juris/liste.jsf?num=C-255/23>>, mn. 7.

15 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.

16 Latvian Economic Court, 19 April 2023, *op. cit.* (n. 14), question 1.

17 CJEU, 6 June 2024, Joined Cases C-255/23 and C-285/23, *AVVA and others / Linte*, para. 38. See also T. Wahl, “ECJ: No Ruling on Defendant’s Right to Participate via Videoconference”, *eucri* 2/2024, 130.

18 CJEU, 06. June 2024, *op. cit.* (n. 17), para. 40 f.

19 ECtHR, 5 October 2006, *Marcello Viola v Italy*, Appl. no. 45106/04, para. 67.

20 See more ECHR Knowledge Sharing platform, *Guide on Article 6 of the European Convention on Human Rights* <[https://www.echr.coe.int/documents/d/echr/guide\\_art\\_6\\_criminal\\_eng](https://www.echr.coe.int/documents/d/echr/guide_art_6_criminal_eng)>, 158, 303; also ECtHR, *Marcello Viola v Italy*, *op. cit.* (n. 19), paras. 63–69; ECtHR, 27 November 2007, *Asciutto v Italy*, Appl. no. 35795/02; ECtHR, 9 November 2006, *Golubev v Russia*, Appl. no. 26260/02; ECtHR,



- 2 November 2010, *Sakniovskiy v Russia*, Appl. no. 21272/03, para. 98.
- 21 Recital 10 of Council Framework Decision 2009/299/JHA, *OJ L 81*, 27.3.2009, 24.
- 22 D. Brodowski, *op. cit.* (n. 8), p. 436 f.; L. Sommerer, *op. cit.* (n. 6), 403, 431 with further references.
- 23 D. Brodowski, *op. cit.* (n. 8), p. 436 f.; L. Sommerer, *op. cit.* (n. 6), 403, 431 with further references.
- 24 D. Brodowski, *op. cit.* (n. 8), p. 439, referring to M. El-Ghazi/A. Hoffmann, "Verwertbarkeit nonverbalen Verhaltens des Angeklagten bei der Urteilsfindung", (2020) *Strafverteidiger (StV)*, 864, 867 f. So far, the ECtHR has not judged on this matter in light of Art. 6(2) ECHR.
- 25 German Federal Constitutional Court (BVerfG), Decision of 14.06.2007 – 2 BvR 1447/05, para. 89; BVerfG, Decision of 15.12.2015 – 2 BvR 2735/14, para. 58.
- 26 D. Brodowski, *op. cit.* (n. 8), p. 438 f.
- 27 But see the reasoning by L. Sommerer, *op. cit.* (n. 6), 403, 419.
- 28 D. Brodowski, *op. cit.* (n. 8), pp. 439 ff. with further references.
- 29 D. Brodowski, *op. cit.* (n. 8), p. 437.
- 30 M. Jahn, in: J.-P. Becker *et al.* (eds.), *Löwe-Rosenberg. Die Strafprozeßordnung und das Gerichtsverfassungsgesetz*, 27th ed., 2021, § 140, mn. 2; M. Jahn/D. Brodowski, in: E. Hilgendorf/H. Kudlich/B. Valerius (eds.), *Handbuch des Strafrechts. Band 7 Grundlagen des Strafverfahrensrechts*, 2020, § 17, mn. 52.
- 31 Art. 64 of Act CLXXX of 2012 on the cooperation with the Member States of the European Union in criminal matters.
- 32 Chapter IV of Act CLXXX of 2012.
- 33 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, *OJ C 197*, 12.7.2000, 3.
- 34 H. Csernák/K. Pencz/Z. Tasnádi/A. Bertaldó, "Az európai nyomozási határozat – vagy más jogsegély? I. – The European Investigation Order – or another legal assistance? I." (2021) 4 *JURA* 51, 79 <[https://jura.ajk.pte.hu/JURA\\_2021\\_4.pdf](https://jura.ajk.pte.hu/JURA_2021_4.pdf)>.
- 35 Art. 11 of Directive 2014/41/EU, *op. cit.* (n. 15).
- 36 Art. 24(2) of Directive 2014/41/EU, *op. cit.* (n. 15).
- 37 Art. 63/C (3) of Act CLXXX of 2012.
- 38 Art. 24(3) and (5) Directive 2014/41/EU, *op. cit.* (n. 15).
- 39 Recital 15 of Directive 2014/41/EU, *op. cit.* (n. 15).
- 40 Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings, *OJ L 280*, 26.10.2010, 1.
- 41 Art. 53(4) of Act CLXXX of 2012.
- 42 Cf. Art. 4(3) TEU.
- 43 Latvian Economic Court, 3 May 2023, *op. cit.* (n. 12), mn. 12.
- 44 Latvian Economic Court, 3 May 2023, *op. cit.* (n. 12), mn. 13.
- 45 Latvian Economic Court, 3 May 2023, *op. cit.* (n. 12), mn. 13.
- 46 Opinion of Advocate General Medina, 18.04.2024, Case C-760/22, *FP and Others*, para. 75.
- 47 See AG Opinion, *op. cit.* (n. 46), paras. 60–63, 65.
- 48 Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation, *OJ L*, 2023/2844, 27.12.2023.
- 49 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *OJ L 191*, 28.07.2023, 118.

# Differential Diagnosis in Online Regulation

## Reframing Canada's "Systems-Based" Approach

Randall Stephenson and Johanna Rinceanu

In February 2024, following Germany's "Netzwerkdurchsetzungsgesetz", the European Union's Digital Services Act, and the United Kingdom's Online Safety Act, Canada exploited its "second mover" regulatory status by introducing its long-awaited Bill C-63. Through its Online Harms Act and related amendments, it proposed an innovative "systems-based risk assessment" model for regulating harmful online content. In this article, the authors argue that any truly "systems-based" approach will benefit from regulatory insights and prescriptions informed by the following two interdisciplinary sources. First, both constitutional and media law scholars endorse stepping outside conventional regulatory models by employing more "context-based" or holistic approaches—a regulatory turn seemingly consistent with Canada's pivot towards an innovative "systems-based" model. Second, exploring further the synergies between law and medicine introduced in our previous Digital Iatrogenesis *eucri*m article, any enhanced framework aimed at "cracking the code" of digital media regulation will benefit from profound insights native to social medicine and diagnostic theory. Besides providing a convincing case for expanding aetiological (and regulatory) inquiry to include social and environmental factors, established principles of medical diagnosis provide a valuable decision-making protocol for present-day regulators. Taken together, leading regulatory and medico-diagnostic scholarship suggests that prevailing "systems-based" models—as epitomised by Canada's proposed Online Harms Act—would appear to function as a "blueprint" for privatised government censorship, providing regulators with the legislative mandate, informational transparency, and compliance authority necessary for regulatory capture. As one of the Internet's "Big Picture" dilemmas, these censorship concerns may yet require reassessment of Europe's current regulatory framework.

## I. Introduction

The Internet and social media have triggered a tectonic shift in our digital “global village”.<sup>1</sup> Discourse production has moved onto a new online medium with a radically different structure and dynamic.<sup>2</sup> Besides creating a revolutionary “participatory” communications model (i.e. shifting from a few-to-many to many-to-many dynamic),<sup>3</sup> a key feature of our digital free speech infrastructure has been the emergence of a small group of powerful privately-owned digital intermediaries—the so-called “Big Five” (Google, Meta (formerly, Facebook), Amazon, Microsoft, and Apple)<sup>4</sup>—who not only effectively “own” and operate the Internet, but function as increasingly decisive arbiters of what information users access online, and what content ultimately reaches the public sphere.<sup>5</sup> Generating unprecedented regulatory challenges, a combination of these influential “new governors”,<sup>6</sup> an increasingly complex digital media infrastructure, and continuing technological advances not only creates tension with existing legal rules and principles,<sup>7</sup> but gives rise to increasing lower-salience *structural* threats to democracy, manifesting in unprecedented global surveillance, manipulation, and control.<sup>8</sup> Regardless of which of the two leading regulatory approaches is championed—viz., the European Union’s predominant “notice-and-action” model or America’s contrasting system of “market self-regulation”—conventional online regulations exhibit near-singular focus on restricting “problematic” online content (e.g. hate speech and misinformation), leaving the accelerating and more disquieting phenomena of mass surveillance and privatised government censorship unaddressed.<sup>9</sup> As we have previously cautioned, without prioritising these structural threats, regulators—much like physicians—risk treating only the symptoms of our increasingly dysfunctional online public sphere, rather than grasping their aetiology of broader tensions, patterns, and interrelationships.<sup>10</sup>

A promising antidote to these growing regulatory challenges is Canada’s evolving “multi-stakeholder” approach, which has been marked by extensive public and expert consultations. Inspired at first by Germany’s popular “notice-and-takedown” model,<sup>11</sup> following widespread criticism of likely encroachments on freedom of expression by Bill C-36 (Canada’s provisional hate speech legislation introduced in 2021), politicians quickly announced plans to go back to the proverbial “drawing board”.<sup>12</sup> Mindful of the need for political and regulatory compromise, Canada’s minority Liberal government proceeded on the sensible expectation that future regulations would not be a straightforward “panacea”, but would comprise only “one piece of a bigger puzzle”.<sup>13</sup> By avoiding a fixed timeframe for introducing their new and potentially more forward-thinking framework, Canada’s regulators vowed instead to take whatever time necessary to meet the challenge of “getting

the legislation right”.<sup>14</sup> On 26 February 2024, following earlier regulatory attempts by Germany, the European Union, and the United Kingdom, Canada exploited its apparent “second mover” status by finally introducing Bill C-63 which, through its Online Harms Act and related amendments, proposes an innovative “systems-based risk assessment” model for regulating harmful content online.

In this article, we argue that despite the Canadian government’s enthusiasm and lofty aspirations, any truly consultative or “systems-based” approach will benefit from regulatory insights and prescriptions informed by the following two interdisciplinary sources. First, the balance of authority of constitutional and media law scholars emphasises the necessity of stepping outside conventional regulatory models by employing more “context-based” and “systems thinking” approaches—a regulatory turn seemingly consistent with Canada’s pivot towards an innovative “systems-based” model. Second, any enhanced framework aimed at “cracking the code” of digital media regulation will benefit from profound insights native to the disciplines of social medicine and diagnostic theory. Besides providing a convincing case for expanding aetiological (and regulatory) inquiry to include the effects of social and environmental signals, established principles of medical diagnosis provide a valuable self-reflexive decision-making protocol for present-day regulators. Taken together, a careful review of “systems-inspired” regulatory scholarship and medico-diagnostic principles suggests that prevailing “systems-based” models—as epitomised by Canada’s proposed Online Harms Act—would appear to function as a “blueprint” for privatised government censorship,<sup>15</sup> providing regulators with the legislative mandate, informational transparency, and compliance authority for regulatory capture that leading scholars have long understood as one of the Internet’s “Big Picture” regulatory dilemmas.<sup>16</sup>

In the end, just as earlier medical debates between germ theorists and proponents of social medicine exposed the importance of host responses and environmental cues to our knowledge of health and illness,<sup>17</sup> contemporary tensions in the field of digital media regulation can shed much-needed light on the dangers of untreated structural threats to the discursive health of our global body politic.

## II. Global Regulatory Approaches

Despite the original aim of cyber-libertarians to create an unfettered online environment, two predominant models of Internet regulation have emerged worldwide, reflecting fundamentally different schools of thought and approaches to freedom of expression.

## 1. “Notice-and-action” model (NetzDG/DSA)

Typified by Germany’s Network Enforcement Act (*Netzwerkdurchsetzungsgesetz* – NetzDG) and Europe’s Digital Services Act (DSA),<sup>18</sup> the “notice-and-action” model is characterised by a relatively strict regulatory approach.<sup>19</sup> This model limits digital platforms’ speech interests by obliging them to delete or block illegal online content within prescribed periods, ranging from 24 hours to seven days. Platforms must also provide an accessible and user-friendly complaints procedure for illegal online content, and are obliged to report potentially criminal content to law enforcement authorities.<sup>20</sup> Importantly, systematic non-compliance leads to severe penalties.

Besides prompting extensive public and private co-optation, this regulatory model has suffered from ambiguous definitions of “illegal” online content: NetzDG, for example, references specific infractions in Germany’s Criminal Code, (e.g. insult and disturbances to the public peace), whereas the DSA introduces a significantly broader definition, not enumerating specific criminal provisions. This definitional ambiguity is ultimately left to digital platforms to resolve—a complex legal assessment that can cause broadly divergent results in each of the EU’s 27 Member States<sup>21</sup>—which places platforms in the unenviable role of powerful gatekeepers at the threshold of human rights.

## 2. “Market self-regulation” (USA)

Canonically associated with the United States of America, the “market self-regulation” model represents a fundamentally different approach to regulating online communications and is characterised by two essential elements. First, platforms are shielded from liability for speech torts committed on their platforms under section 230 of the Communications Decency Act (CDA). Second, the US Constitution provides an enlarged scope of protection for “offensive” speech under the First Amendment, including hate speech.<sup>22</sup> In effect, “market self-regulation” allows platforms to determine—with minimal state interference and risk of liability—what content to carry and remove. Compared to the “notice-and-action” model, free-speech restrictions under “market self-regulation” are not imposed by government legislators, but by modifying platforms’ content moderation policies, or Terms of Use.

## III. Canada’s “Systems-Based” Regulatory Proposal

Compared to the EU and America, Canada has embraced a novel “multi-stakeholder” approach to resetting its regulatory framework. In its consultative journey, the Canadian gov-

ernment has pivoted from conventional “notice-and-action” models to a more “systems-based” approach. By imposing a “duty to act responsibly” on digital platforms, Canada’s new Bill C-63 seeks to provide Canadian regulators with information and greater transparency about key *ex ante* and systemic decision-making processes taking place outside and upstream of more conventional models of *ex post* content review and error correction.

### 1. Moving from a “notice-and-takedown” to a “systems-based” model

Canada’s “multi-stakeholder” approach is notable for two particularities. Besides moving from a conventional “notice-and-takedown” to a more “systems-inspired” regulatory approach, Canadian legislators have shown a distinct preference for combating harmful online content rather than heeding and prioritising concerns expressed by the public and experts alike with rising censorship and more structural threats to democratic governance.

#### a) Public consultation – concerns with privatised government censorship

Following its abandonment of Bill C-36, the Canadian government began public consultations soliciting Canadians’ views on regulating harmful online content. From July to September 2021, the government requested written submissions from the public and tech-industry on its original “notice-and-takedown” regulatory model (i.e. Bill C-36), and associated technical and discussion papers.

While public respondents unanimously accepted the necessity of state intervention—as opposed to “market self-regulation”—far fewer supported the proposed legislative framework as a whole. Importantly, from the very beginning of Canada’s extensive regulatory planning, a broad cross-section of stakeholders expressed six main or “prominent” concerns on the dangers of censorship and the over-regulation of online content, relating to: (1) definitional clarity of harmful content; (2) proactive monitoring; (3) expedited takedown requirements (e.g. 24-hour rule); (4) economic drivers of platform content moderation; (5) bureaucratic overreach; and (6) transparency and accountability reporting duties.

First, respondents criticised the lack of definitional detail for online harms, warning that overly broad definitions would invite bias and could have a chilling effect that might “create a broader trend toward over-censorship of lawful expression writ large”.<sup>23</sup> Second, quite aside from its present-day reality, stakeholders expressed concern

that a general proactive monitoring obligation on platforms would be extremely problematic as it would “likely [...] amount to pre-publication censorship”, and ultimately “operate as a *de facto* system of prior restraint”.<sup>24</sup> Third, many respondents called for removing the 24-hour take-down rule borrowed from Germany’s NetzDG, arguing that “it would incentivize platforms to be over-vigilant and over-remove content [...]”.<sup>25</sup> Fourth, multiple respondents keenly observed that rather than focus exclusively on content moderation, regulators should target “the *economic* factors that drive platform design and corporate decision making”,<sup>26</sup> including other “[...] *structural* factors like advertising practices, user surveillance, and algorithmic transparency [...]”.<sup>27</sup> Fifth, despite the overall enthusiasm for urgent regulatory intervention, stakeholders questioned “the number of regulatory entities, emphasizing potential overlaps in authority and the sheer size of the proposed bureaucratic structure dedicated to ‘censoring’ online expression”.<sup>28</sup> Sixth and finally, moderate concern was expressed about transparency and accountability requirements. As one of the most powerful governance tools, respondents hoped that mandated and audited transparency could operate as “important safeguards to mitigating the regime’s potential for over-removal and censorship”.<sup>29</sup>

### b) Expert consultation – pivoting to a “systems-based” regulatory approach

The second phase of Canada’s “multi-stakeholder” approach involved the solicitation of expert advice. In March 2022, an Expert Advisory Group on Online Safety (EAG) was convened composed of Canadian experts in platform governance and content regulation, online harms, civil liberties, informatics, and national security. Its dual mandate was to provide insights and recommendations on how best to design a legislative and regulatory framework to address harmful online content, and to advise on “how to best *incorporate* the feedback received during the national consultation [...]”.<sup>30</sup> Like ordinary Canadians, the EAG endorsed state regulation, proclaiming that online safety “cannot be left to the good graces of industry players”.<sup>31</sup>

Remarkably, while two of the five censorship concerns voiced in the public consultation were taken up by the EAG (i.e. definitional clarity and proactive monitoring), the remaining three worries were effectively downplayed or disregarded. While expert comment was anonymised by the government, the issue of generalised or proactive platform monitoring was mentioned repeatedly in two of the ten EAG workshops. When advising on the appropriate types of regulatory content, multiple experts worried that “whatever framework is chosen, it would be *critically important* that

it not incentivize a general system of monitoring”.<sup>32</sup> When experts turned their minds to evaluating the new regulatory approach under consideration, some stressed that “there is a risk that a systems-based approach could *indirectly* promote a system of general monitoring”, advising that “each legislative provision must be scrutinized to ensure no general monitoring obligation exists [...]”.<sup>33</sup> Moreover, besides confirming earlier concerns with definitional uncertainties regarding harmful content,<sup>34</sup> the EAG expanded these to include the new framework’s proposed “duty to act responsibly”.<sup>35</sup> Experts cautioned that “if regulated services are not told *how* to comply with their duty to act responsibly, the systems they put in place might be rudimentary and result in *blunt over-regulation* [...]”.<sup>36</sup>

Notwithstanding other minor and less-specific references to freedom of expression and government censorship, the EAG took particular interest in regulating disinformation, with most experts agreeing that “the Government *cannot* be in the business of deciding what is true or false online, or of determining intent behind creating or spreading false information”.<sup>37</sup> In a statement reminding Canadians of the grave dangers of regulatory capture, most EAG members insisted categorically that “the Government [cannot] censor content based on its veracity, *no matter how harmful*”.<sup>38</sup> Finally, unlike the more critical and far-reaching citizen concerns with the economic drivers of online censorship—which was more amenable (at least in theory) to acknowledging the economic foundations of over-filtering and over-blocking—some members of the EAG highlighted the importance of only the financial and economic drivers of *disinformation*. Apparently unwilling or reluctant to contemplate the relationship between economic motives and online censorship, these experts nonetheless suggested that successful answers to disinformation may lie beyond regulatory reach if advertising law and practices were not altered to effectively “demonetize disinformation”.<sup>39</sup>

At last, apart from these relatively few and abridged regulatory concerns, previously vetted worries with rising regulatory capture and privatised government censorship did not appear to resonate as strongly with Canada’s expert panel.

### c) Citizens’ assemblies on democratic expression and national roundtable discussions

The final phases in Canada’s lengthy consultative process involved important input from the Canadian Commission on Democratic Expression and the Department of Canadian Heritage, which provided vital feedback on the EAG and the state of regulatory input to date. Importantly, as with initial public consultations, significant concerns were again

expressed about the dangers of censorship and avoiding over-regulation of speech interests.

#### aa) “Capstone” assembly on democratic expression – protecting dissenting opinions

Following the EAG’s counsels on how best to design a regulatory framework for addressing harmful online content, Canadian Heritage requested a third and final Citizens’ Assembly on Democratic Expression to review and respond to the EAG’s suggestions and all work that had preceded its input and efforts. At stake in the minds of many members of this “capstone” assembly was nothing less than the future of Canadian democracy.<sup>40</sup>

Although reflecting the emerging consensus on the urgent need for state regulation, this second public consultation again acknowledged the vital importance of avoiding censorship and over-regulation of free expression. First, Assembly members expressed concern that “online users [...] be able to share *dissenting* or *unpopular* opinions”,<sup>41</sup> and that any risk-based model contain appropriately “strong whistle-blower protections”.<sup>42</sup> Second, comparable to feedback from the first public consultation in 2021, Assembly members pointed out the detrimental economic implications and overall costs of digital platforms’ business models and over-reliance upon click-through ads in our digital “attention economy”, warning that platforms’ overriding “goal of profit from advertising sales comes at a detrimental cost, and with great disregard, to the *well-being of our society*”.<sup>43</sup>

#### bb) National roundtable discussions – misapprehending economic regulatory motives

Finally, in July 2022—shortly after the EAG completed its work—the Canadian government conducted 19 nationwide roundtables to incorporate victim and platform perspectives on the EAG’s advice and recommendations.<sup>44</sup>

As confirmed throughout the consultative process, consensus was again reached over the urgent need for state regulation of harmful online content. Still, evidencing an overall concomitant fading of concern with censorship and over-regulation, participant feedback was limited to passing references to the dangers of government involvement in regulating disinformation, and the regulatory implications of platforms’ business models. Echoing the EAG’s insistence that the government cannot be deciding what is “true” or “false” online, roundtable participants were greatly uneasy “at the notion that the government should be the entity deciding what material constitutes misinformation

and disinformation”.<sup>45</sup> Importantly, this feedback provided yet more evidence of persisting confusion over the scope of effects of economic factors on content moderation. Many participants expressed concern only about their impact on delaying removal of harmful online content, voicing scepticism over “the willingness of social media platforms to self-regulate content [...] due to the site traffic and revenue the content can generate”, and “platforms prioritizing profits rather than monitoring content [...]”.<sup>46</sup> Besides implicitly endorsing proactive monitoring, overlooked again was the impact of economic drivers on over-filtering and over-blocking, and the more veiled dangers of privatised government censorship.

## 2. Bill C-63: Canada’s latest regulatory framework

On 26 February 2024, Canada introduced Bill C-63<sup>47</sup>—its long-awaited regulatory framework for addressing harmful online content. Besides amending (among others) the Criminal Code and the Canadian Human Rights Act (CHRA), Bill C-63 introduced the Online Harms Act, intended to make good on its earlier promise to Canadians of “getting the legislation right”.

Besides imposing sensible duties to protect children and to make non-consensually distributed intimate images and child pornography inaccessible in Canada within 24 hours, the Online Harms Act imposes on digital platforms a “duty to act responsibly” by implementing measures to mitigate the risks that users will be exposed to harmful content. This negligence-based duty requires (above all) that platforms submit regular Digital Safety Plans—containing detailed risk assessments, mitigation strategies, and evaluations of their efficacy—to a newly established Digital Safety Commission of Canada, whose mandate would be administering and enforcing the Act. Besides this governing regulatory body, the proposed Act also establishes a Digital Safety Ombudsperson to support users of regulated services and to advocate for the public respecting systemic online safety issues, and a Digital Safety Office of Canada to provide administrative support to the two newly-created agencies.

Consistent with Canada’s regulatory focus on combating harmful online content, Bill C-63 includes three vital harm-related provisions. First, the Online Harms Act adds two additional categories of harm (i.e. child bullying and self-harm) to the following five categories discussed throughout Canada’s consultative process, namely: (1) content that sexually victimises a child or revictimises a survivor; (2) intimate content communicated without consent; (3) content that foments hatred; (4) content that incites violent extremism



or terrorism; and (5) content that incites violence. Second, Bill C-63 amends the Criminal Code by: (1) proposing a long-awaited definition of “hatred”; (2) creating a controversial standalone “hate crime” offence (liable to imprisonment for life) that applies to existing criminal offences and parliamentary acts motivated by hatred;<sup>48</sup> (3) increasing penalties for existing hate crimes; and (4) instituting a new “peace bond” designed to *prevent* the commission of hate crimes and offences. Third and finally, Bill C-63 aims to reinstate Section 13 of the CHRA to make it a discriminating practice “[...] to communicate or cause to be communicated hate speech by means of the Internet or any other means of telecommunication [...]”;<sup>49</sup> thereby broadening the scope of remedies for victims of online harm.

In the end, notwithstanding the broad range of public and expert concern voiced over the dangers of censorship and over-regulation of speech interests during its extended consultation process, Canadian legislators appear to have focused disproportionately on harmful content at the expense of addressing lower-salience structural threats to democratic governance.

#### IV. Differential Diagnosis in Online Governance

After introducing Canada’s new “systems-based” framework, Part IV demonstrates that reliable indications as to its optimal form and content can be discerned from two key interdisciplinary sources: (1) constitutional and media law scholarship emphasising the necessity of employing “context-based” and “systems thinking” approaches to online regulation; and (2) profound regulatory insights native to the fields of social medicine and diagnostic theory. Taken together, these confirm that future regulatory models must openly embrace synthetic enquiry and careful avoidance of overly-reductionist approaches to online dysfunctions.

##### 1. “Systems thinking”: Stepping outside conventional regulatory models

The nature and limitations of Canada’s “systems-based” model can be first gathered from leading constitutional and media law scholars who collectively endorse: a) adopting more structurally sophisticated means of integrating socio-technical-legal elements into regulatory theory and design; b) adopting novel “context-based” approaches to digital platform liability; and c) reframing content moderation in terms of “systems thinking”. Despite developing such insights within relatively narrow fields of reference, these scholarly efforts assist greatly in envisioning an integrative perspective on online regulation.

##### a) Multi-ordinal mapping of digital information flow

One of the most challenging aspects of ongoing technological advances in cyberspace has been reconciling their disruptive regulatory effects (and failures), and identifying the details and guiding principles for an effective global framework of Internet governance.<sup>50</sup> Central to this aim has been confronting the “shaky” theoretical grounds underlying current regulatory structures and—given the Internet’s clash with the principle of territoriality—embedding technological advances into an effective global system.<sup>51</sup> Despite a lack of consensus about the conceptual grounds of online regulation, scholars *have* agreed on an important feature about its structural complexity. Reflecting hard-won lessons of legislators worldwide, commentators insist that “a single concept cannot explain the complex structure of cyberspace” and hence resort to some form of “systems-inspired” or “interrelated thinking seems *unavoidable*”.<sup>52</sup>

##### aa) Murray’s three-dimensional “complexity matrix”

An important early contribution to defining possible future perspectives on Internet governance was provided by *Andrew Murray*.<sup>53</sup> Writing in an earlier online era focused on optimising digital information flow, *Murray’s* principal insight was that cyberspace is a complex, even *chaotic*, environment that requires legislators to employ a “[...] more cohesive, measured, prudent and non-interventionist approach”.<sup>54</sup> Distinguishing his pioneering regulatory theory from earlier “cyber-libertarian” and “cyberpaternalist” models, *Murray’s* “complexity thesis” rejected their joint assumption of a static regulatory setting by endorsing a more *dynamic* model capturing the complexities of State and private sector actors. *Murray* advised that by recognising parties’ dual roles as “regulator” and “regulatee”—and adopting a more dynamic “systems-inspired” view of the regulatory environment—legislators “[...] are offered the opportunity to produce effective *complimentary* regulation”.<sup>55</sup> Accordingly, in his bid to minimise disruption and to harmonise regulatory efforts with policy outcomes—both aims resonant with autopoiesis theory—*Murray’s* contrasting model of “*symbiotic regulation*” endorsed a distinctive protocol harnessing the complex relationships between the various regulatory actors.<sup>56</sup>

Inspired by these biological and remedial concepts, *Murray* introduced a novel three-dimensional matrix for structuring and regulating complex, digital media environments.<sup>57</sup> According to *Murray*, successful online regulation requires that the *complexity* of the broader media environment be accurately mapped, including the communications networks already in place.<sup>58</sup> Recognising that “all actors in the

regulatory environment play an active role [...],<sup>59</sup> interventions in such complex networked systems are fundamentally *indeterminate* in that “[...] the complexity of the matrix means that it is impossible to predict the response of any other point [...]”.<sup>60</sup> This however does not mean that cyberspace is fundamentally unregulable. Quite the contrary. Owing to the overall “malleability of its environment”,<sup>61</sup> Murray insisted that our online environment is highly amenable to regulation using a reflexive three-step process.

The first step is to produce a dynamic model of the regulatory environment, being careful to record all relevant parties and to map their primary communication dynamics. The focus is not on capturing actual content, but on mapping the *relationships* between actors well enough to “anticipate the regulatory *tensions* that are likely to arise [...]”.<sup>62</sup> Second, based on the accuracy and comprehensiveness of this initial environmental modeling, regulatory interventions can be optimally formulated to *anticipate* and *avoid* regulatory tensions between its main actors, thereby offering a positive communication “to the subsystems, or nodes, within the matrix [...]”.<sup>63</sup> Murray further specified that these regulatory interventions are “intended to harness[] the natural communications flow by offering to the subsystems, or nodes [...] a positive communication that encourages them to support the regulatory intervention”.<sup>64</sup> Third, regulatory interventions must then be tested by monitoring positive and negative nodular feedback. According to Murray, whether aiming to reinforce already successful regulations, or to engender modifications directed at enhancing deficient regulatory outcomes, “[...] regulator[s] should be prepared in light of this feedback to make alterations in their position and to continue to monitor feedback on each change [...]”.<sup>65</sup> By following this three-stage process regulators are, according to Murray, best equipped “to design successful [...] interventions in the most complex regulatory environment”.<sup>66</sup>

At last, while criticised as being “difficult to implement” and “[...] impossible to adequately carry out”,<sup>67</sup> Murray’s “complexity thesis” nonetheless remains a vital early contribution to confronting rising challenges of regulating complex networked environments.

### b) “Context-based” approaches to regulating platform liability

A second indication as to the nature and limitations of Canada’s “systems-based” regulatory model can be gathered from examining the underlying bases of platform liability. Several forward-thinking scholars have endorsed a broad array of “context-based” models.

#### aa) Lavi’s “descriptive social technological” model

A significant early contribution to online regulatory theory and design in the social media era was Michal Lavi’s innovative “context-based” model.<sup>68</sup> Aiming to reconcile tensions between prevailing legal rules and the attribution of liability for online speech torts, Lavi noted presciently that our modern-day digital media ecology places the right to free expression and its underlying justifications decidedly in “a new light”.<sup>69</sup> Concerned particularly about the “chilling effect” of holding content providers liable for speech torts committed on their platforms, Lavi cautioned that a single, overarching regulatory approach would be “insensitive to different online *contexts* and lead to distortions and improper [regulatory] consequences”.<sup>70</sup>

In response, Lavi endorsed an innovative “descriptive social technological” model erected on a three-level conceptual taxonomy for matching liability rules to an overarching sociological criterion that measures the *strength of social ties* and their potential for causing harm. By dividing digital platforms into three categories with increasingly strong social ties—(1) “freestyle platforms” (e.g. Yahoo! Message board); (2) “peer production platforms” (e.g. Yelp and other user review sites); and (3) “deliberation and structuring communities” (e.g. Meta (formerly Facebook, X (formerly Twitter), and other social networks)—in simplest terms, Lavi proposed a model of “differential liability regimes”,<sup>71</sup> arguing that since platforms’ various technical and functional capabilities influence speech-related harms *differently*, liability should increase concomitantly with each platform’s potential for doing so. That is to say, whenever the severity of harm is low and there is a substantial likelihood for private ordering, legal regulations are unnecessary. But where the social media context increases harm to external victims and results in a failure of private ordering, content providers should not be granted legal immunity (e.g. under section 230 CDA), and should be subject to some form of “notice-and-takedown” procedure.<sup>72</sup> Consistent with earlier warnings against the impracticality of Murray’s “complexity thesis”, Lavi advised that her regulatory model—along with “context-based” approaches generally—might provide courts and legislators with a more practical alternative—“[...] a simple *rule of thumb* for defining content providers’ scope of liability”.<sup>73</sup>

Importantly, the regulatory implications of Lavi’s “context-based” model extend well beyond issues of doctrinal coherence. Reiterating concerns of lower-salience structural threats to democracy advanced by leading free speech scholars like Jack Balkin,<sup>74</sup> Lavi stressed that the fundamental motive for platform content moderation is “*econom-*

ic and not driven by legal considerations”.<sup>75</sup> This point is critically important not only for “optimally balancing” competing policy rationales underlying platform liability, but to identifying the “root causes” of over-filtering, over-blocking, and acknowledging the potential for and dangers of privatised government censorship—*structural* concerns vital both to the maintenance of a healthy marketplace of ideas, and for effectively holding power to account.<sup>76</sup>

At last, besides the utility of *Lavi’s* model for ensuring doctrinal coherence and reform, it also attests to the regulatory dangers of ignoring the discomfiting reality that the “economic logic” driving platform content moderation too often conflicts with human rights norms, particularly free speech and its vital “checking function” rationale.<sup>77</sup>

#### bb) *Sander’s “structural” human rights law model*

A second valuable contribution to online regulatory theory and design in the social media era was *Barrie Sander’s* “structural” human rights law model.<sup>78</sup> Building on many of the “context-based” regulatory insights noted earlier, *Sander* argued that shifting to a more structural conception of human rights law would—by broadening *Lavi’s* approach to platform liability even further—require “[...] a more *holistic* and *evidence-based* approach to the design of intermediary liability laws that strives to account for the *systemic effects* of such frameworks on online expression”.<sup>79</sup> Calling for greater state protection of free speech, *Sander’s* “structural approach” to regulating online content requires that sufficiently “[...] robust mechanisms of transparency, due process, accountability and oversight are embedded in platform moderation systems [...]”,<sup>80</sup> including government and cross-platform collaborations.

By examining content moderation (and data protection) liability within the wider context of rising *accountability deficits* pervading our digital media ecology,<sup>81</sup> *Sander* took aim at the prevailing “marketized” model of human rights law in our “increasingly, privately controlled, neoliberal communication sphere”.<sup>82</sup> In particular, *Sander* argued that a marketised conception premised on the *laissez-faire* notion of “[...] protect[ing] individual choice and agency against state intervention” is problematic for two reasons.<sup>83</sup> First, it endorses a form of abstract individualism that “[...] neglects power asymmetries between individual users and other actors that participate in the social media ecosystem [...]”.<sup>84</sup> Second, it pays limited attention “[...] to the *systemic effects* of state and platform practices on the social media environment as a *whole*”.<sup>85</sup>

In response, *Sander* endorsed a “structural” conception of human rights law, one typified by “a greater openness to *posi-*

*tive* state intervention as a means of safeguarding public and collective values such as media pluralism and diversity”.<sup>86</sup> By doing so, *Sander* aimed to not only contest the use of human rights discourse in the realm of social media governance,<sup>87</sup> but to “[...] begin to close the accountability deficits associated with content moderation [...]” that increasingly threaten our democracies.<sup>88</sup> While leaving the regulatory details unspecified, *Sander’s* commitment to preserving the “functionality” of our digital public sphere provides important normative grounds for expanding our regulatory toolbox to include “common carrier” doctrine for mitigating platform censorship and increasing the quantity and diversity of democratic discourse.<sup>89</sup>

In the end, when interpreted in light of *Murray’s* three-dimensional “complexity matrix” and *Lavi’s* “descriptive social technological” model of platform liability, *Sander’s* model again attests to the vital importance for online regulators of turning their minds to the *broader* regulatory environment—including its primary stakeholders’ economic motives and discursive predilections—for clues to calibrating our regulatory interventions to better promote international human rights, domestic policy goals, and the health of our online environment.

#### c) Content moderation as “systems thinking”

A third indication as to the nature and limitations of Canada’s “systems-based” model can be inferred from scholarship endorsing a “second wave” of more sophisticated regulatory frameworks for online content moderation. Looking to step outside overly reductionist models, legal scholars have continued to incorporate key concepts and insights from systems theory to optimise our understanding and regulation of today’s digital media environment.

#### aa) *Douek’s “monitored self-regulation” model of content moderation*

A third notable contribution to online regulatory theory and design in the social media era was *Evelyn Douek’s* ambitious reframing of content moderation (and its regulatory dynamics) in terms of “systems thinking”.<sup>90</sup> Arguing that today’s content moderation models (e.g. “notice-and-action” and “market self-regulation”) are equally outdated, misleading, and incomplete,<sup>91</sup> *Douek* claimed that the “blind spots” and mistaken assumptions of this “standard” regulatory picture—a “first wave” of regulation focused incorrectly on *ex post* review of *individual* online posts and error correction—must be updated and replaced with a “second wave” capturing the underlying “patterns and interrelationships” of our modern regulatory landscape. As *Murray* foresaw a generation earlier, *Douek* maintained that content moderation is ultimately a complex and dynamic system of “mass speech administration”,<sup>92</sup> which re-

quires wide-ranging procedural design interventions focused more on “[...] systems rather than individual cases, on wholes and interrelationships rather than parts, and on ‘patterns of change rather than static snapshots’”.<sup>93</sup>

Starting from the sensible bases that “there will never be agreement on what constitutes ‘good’ content moderation”<sup>94</sup> and—perhaps most importantly—that “the status quo of private companies determining matters of [...] public significance without any form of accountability, transparency, or meaningful public input is *inadequate*”,<sup>95</sup> Douek’s main regulatory objective involves achieving “meaningful accountability” by reframing content moderation as a complex and dynamic *administrative* system.<sup>96</sup> Endorsing a self-styled “substance-agnostic” approach,<sup>97</sup> Douek’s regulatory framework draws on familiar “principles and practices of administrative law”,<sup>98</sup> focused more on “key *ex ante* and systemic decision-making” taking place *outside* and *upstream* of the standard picture’s familiar “assembly line” of *ex post* individual review and error correction. Rather than providing “substantive” reforms, Douek’s overriding objective of mitigating online “accountability deficits”—a policy aim endorsed earlier by Sander—requires adopting two coordinate sets of structural and procedural reforms.

First, any proper system of “mass speech administration” must begin by restructuring internal platform moderation bureaucracies to avoid unreported bias and to incentivise neutral enforcement of their Terms of Use.<sup>99</sup> Douek’s “separation of functions” principle hence requires *intra*-corporate separations of personnel and functions “that aim to ‘eliminate the *incentives* that would make [biased] conduct possible or likely in the first place’”.<sup>100</sup> Second, rather than relying on “user-initiated complaints in individual cases”,<sup>101</sup> a more comprehensive governance framework must authorise a suitable regulatory body—as reflected by Canada’s proposed Digital Safety Commission—to operate an “*external channel*” for fielding complaints and conducting its own investigations. Third, to best facilitate regulatory oversight of complex content moderation systems, platforms should be required “to disclose the nature and extent of involvement of *outside* decisionmakers in their content moderation [...]”,<sup>102</sup> including external “fact-checkers” and (at least in theory) government agencies. Lastly, as accepted by Canadian legislators, Douek proposed a scheme of regular platform reporting obligations (i.e. Digital Safety Plans) *designed* to expose “the broader functioning of their [content moderation] systems”,<sup>103</sup> which purports only to improve accountability and to prevent regulators from “legislating in the dark”.<sup>104</sup>

Besides these structural reforms, Douek argued that optimising regulatory accountability requires digital platforms

to comply with three *procedural* fiats. First, while admitting that platform self-reporting “may *sound* like a feeble form of accountability”,<sup>105</sup> and that the “[e]mpirical effects of speech regulation are deeply contested”,<sup>106</sup> platforms should nonetheless produce “annual content moderation plans and compliance reports”.<sup>107</sup> Besides forcing them “to think proactively and methodically about potential operational risks”,<sup>108</sup> as illustrated by Canada’s proposed Digital Safety Plans, Douek maintained that such disclosures can benefit regulatory efforts by: (1) creating a “paper trail” of platform decision-making that “facilitat[es] future review and accountability”;<sup>109</sup> (2) facilitating policy learning by encouraging “cross-industry reporting” and formulating “general compliance standards” or “best practices”;<sup>110</sup> and (3) much like Canada’s own consultative approach, facilitating public involvement through “multi-stakeholder” engagement into proposed regulations.<sup>111</sup> Regardless of their efficacy, Douek sensibly insisted that as “a necessary first step to more sweeping reform”, we must first admit that “[t] here is [...] no way of currently knowing what platforms have been doing, what works, and what doesn’t”.<sup>112</sup>

Douek’s second procedural proposal also aimed to improve informational transparency, in this case by requiring platforms both to demonstrate that “they have quality assurance [...] measures in place for their decision-making systems”<sup>113</sup>—a core *internal* administrative law requirement—and to subject such self-assurances of “quality” to “independent auditing”.<sup>114</sup> As Douek rightly cautioned, without independent verification, such “[...] transparency reports could be as accurate as Enron’s financial statements [...]”.<sup>115</sup> A third and final procedural recommendation would require platforms to offer an “aggregated review mechanism[]”.<sup>116</sup> Instead of mandating appeals and procedural protections for individual online users, Douek insisted that to better identify and address *system-wide* trends, patterns, and failures, platforms should “review, as a *class*, all adverse decisions in a certain category of rule violation over a certain period [...]”.<sup>117</sup> Drawing on analogies to the EU’s data protection regime (i.e. General Data Protection Regulation), Douek professed that these structural and procedural proposals together amounted to a model of “monitored self-regulation”, one that is more dynamic, better at leveraging the particular capacities of private and public actors, and can generate a virtuous cycle of continuous iterative improvements.<sup>118</sup>

In the end, despite Douek’s worthy aim of prompting a “second wave” of content moderation theory and regulatory design, many important aspects of her framework remain *underdefined* extensionally (e.g. capturing the extent of regulatory activity in our *global* public sphere),<sup>119</sup> and significantly *undertheorised*—ironically in the areas of “sys-



tems-theory” and accountability scholarship.<sup>120</sup> Owing to perfunctory engagement with these vital foundational materials—and adopting an unnecessarily narrow view of “digital platforms” as the main unit of regulatory analysis—*Douek’s* model leaves the following broader regulatory issues unexamined: (1) the rising *structural* threats to democracy posed by the Internet’s ad-based business model, including its impact on over-filtering and over-blocking, and its *overall effects* on the quantity and quality of democratic discourse; and, (2) the implications of a “systems-based” model for facilitating regulatory capture and sanctioning (perchance unintentionally) privatised government censorship.

## 2. A way forward: Regulatory insights from social medicine and diagnostics

Despite these residual scholarly gaps, perhaps the most valuable lesson that has emerged from our review of “systems-inspired” models is harnessing their collective capacity for optimising regulatory “*diagnosis and improvement*”—an important remedial goal of *Douek’s* model.<sup>121</sup> Taking up this implicit mantle, further indications as to the nature and limitations of Canada’s proposed regulatory model are afforded by expanding our inquiry into the instructive parallels between the legal and medical sciences.

### a) Insights from social medicine and theoretical biology

As we have maintained in the past,<sup>122</sup> any regulatory framework aimed at “cracking the code” of online communications will benefit from exploring the considerable synergies between law and medicine.<sup>123</sup> Recommending this same source of interdisciplinary insight when searching for suitable regulatory interventions in cases of constitutional limitation or infringements on liberty, US Supreme Court Justice *Benjamin Cardozo* encouraged both courts and legislators alike to increasingly turn to “[...] *medicine*—to a Jenner or a Pasteur or a *Virchow* or a Lister as freely and submissively as to a Blackstone or a Coke”.<sup>124</sup> Poised on the crest of revolutionary twentieth-century advances in theoretical physics, Justice *Cardozo’s* open-minded views have since only gained in currency in light of powerful insights generated by these new scientific paradigms within the fields of social medicine and theoretical biology.

#### aa) Importance of *social and environmental signals to public health regulation*

One specially revealing nineteenth-century German medical anecdote (and pioneering medical figure) bears mention. It concerned a typhus epidemic that broke out in the winter of

1847 in Upper Silesia, an economically depressed Prussian province. The epidemic coincided with a famine, and conditions deteriorated so badly that government intervention became necessary. Following time-honoured practice, an outside expert was appointed to survey the situation and submit a regulatory report. The individual chosen for this seemingly routine task was the physician *Rudolf Virchow*, then aged 26 years, and a junior lecturer in pathology at the Charité Hospital in Berlin.

The report based on his three weeks’ observation was revolutionary for its time and even now sets a standard for attempting to understand and *change* the social conditions that produce disease. Conspicuously, *Virchow’s* ‘medical’ proposals were quite limited. Since he based the origins of ill health in broader social conditions, the most reasonable regulatory approach to addressing the Upper Silesian ‘epidemic’ was to identify and alter the underlying factors that permitted it to occur. *Virchow* reasoned:

Don’t crowd diseases point everywhere to deficiencies of society? One may adduce atmospheric or cosmic conditions or similar factors. But never do they alone make epidemics. They produce only where due to bad social conditions people have lived for some time in abnormal situations. Typhus would not have spread epidemically in Upper Silesia if there had not been a physically and mentally neglected people [...].<sup>125</sup>

Evidencing a growing awareness of the complex interrelationships between medicine, social conditions, and political reform, *Virchow* later insisted that if medicine was to fulfill its great task, then it must enter the public realm, famously declaring:

Medicine is a social science, and politics is *nothing else but medicine on a large scale*. Medicine, as a social science, as the science of human beings, has the obligation to point out problems and to attempt their theoretical solution: the politician, the *practical anthropologist*, must find the means for their actual solution [...].<sup>126</sup>

Insisting that “[t]he physicians are the *natural attorneys of the poor*, and the social problems should largely be solved by them”,<sup>127</sup> *Virchow* envisioned a medical profession that obliged physicians to investigate the complex relationships between socio-political stressors and corporeal experience. *Virchow’s* intriguing reversal of the traditional roles of doctors and lawyers was borne from a deep conviction that medicine’s clinical realities must inform society’s organisation and structure, predominantly through careful design of its laws and regulations. Stressing their importance as society’s dominant prescriptive force, *Virchow* stated: “If medicine is the science of man both healthy and ill, which after all it should be, *what other science could then be more appropriate to deal with law-making*, in order to *apply* the laws that are given in mankind’s nature to the foundations of the organization of society?”<sup>128</sup>



At last, while *Virchow's* inquiries into the social origins of illness were to help establish the interdisciplinary scientific field of “social medicine”, these issues quickly fell from sight owing to more reductionist scientific developments that shaped the course of medicine during the late-nineteenth century—particularly the germ theory of disease.<sup>129</sup>

### bb) The *biopsychosocial* response: A “systems-based” paradigm of health and illness

The urgency for developing a new medical paradigm responsive to such diagnostic blind spots was reinforced by *George Engel*.<sup>130</sup> In *Engel's* view, medicine was in crisis because of its adherence to a disease model that was no longer adequate for its scientific tasks and social responsibilities.<sup>131</sup> Like *Virchow* before him, *Engel* hoped for an epistemological shift in medical science focused on greater *interaction*, with renewed emphasis on defining adaptive genetic and epigenetic limitations as they are set by broader social and environmental signals. Arguing for a revolutionary “systems-inspired” biomedical paradigm—one typified by a transactional, holistic, analogical, and probabilistic approach—*Engel* effectively confirmed *Virchow's* more tentative causal inferences, instructing:

No linear concept of etiology is appropriate; rather, the pathogenesis of disease involves a series of negative and positive feedbacks with multiple simultaneous and sequential changes potentially affecting any system of the body. The central nervous system is so organized that a reciprocal interrelationship between the mental apparatus and the rest of the body in the pathogenesis of disease states and maintenance of health is not only possible but *inevitable*.<sup>132</sup>

Among its implications, *Engel's* general systems theory-inspired “biopsychosocial” model requires physicians to explore complex relationships between social stressors and bodily experience, to study how the corporealisation of cultural experience occurs, and to explore humanity's adaptive limits to rising levels of immunological stressors. Reflecting the “systems thinking” that led *Rudolf Virchow* to designate nineteenth-century physicians “the natural attorneys of the poor”,<sup>133</sup> this new model implicated physicians in wider political debates from which modern conceptions of suffering and disease often insulate them, a point shown by containing suffering within the sole rubric of prevailing (and potentially misleading) microbiological and genetic disease models.<sup>134</sup>

In the end, *Engel* anticipated that as the social bases of health and illness were gradually revealed, new avenues of research could be opened in precisely the way that *Thomas Kuhn* had in mind—generating a “systems-inspired” paradigm shift in medical science that might through its example advance broader socio-political regulations.<sup>135</sup> That is,

*Engel's* “biopsychosocial” paradigm might yet inspire and foster amongst today's regulators a similar perspectival shift in global online governance—in this case, to a more scientifically probing and less ideologically encumbered and contextually reductionist “systems-inspired” approach.

### b) Regulatory insights from medical diagnostics

Besides these structural insights from social medicine and theoretical biology, valuable clues for designing “systems-inspired” regulatory models can also be grasped from the principles and methods of medical diagnostics.

#### aa) The diagnostic process: “Clinical reasoning” in conditions of uncertainty

Instructive synergies between “systems-based” regulatory approaches and the principles and practices of medical diagnosis can be shown by analysing the latter's three conceptual pillars.

First, and above all, diagnosis is a *process*.<sup>136</sup> As with “systems-based” models committed to optimising “learning and iterative” regulatory outcomes, medical diagnosis consists of a similarly cyclical and “continuous process of information gathering, integration, and interpretation [that] involves hypothesis generation and updating prior probabilities as more information is learned” about *hidden* dysfunctions.<sup>137</sup> Moreover, similar to regulatory measures directed at rectifying dysfunctions in complex networked environments, the diagnostic process encompasses a self-reflexive method of “modification and refinement” that operates under conditions of regulatory *uncertainty*.<sup>138</sup> As Professor *Jerome P Kassirer*, MD explained:

Absolute certainty in diagnosis is *unattainable*, no matter how much information we gather, how many observations we make, or how many tests we perform. A diagnosis is a hypothesis about the nature of a patient's illness, one that is derived from observations by the use of inference. As the inferential process unfolds, our confidence as [clinicians] in a given diagnosis is enhanced by the gathering of data that either favor it or argue against competing hypotheses. Our task is *not* to attain certainty, but rather to *reduce* the level of diagnostic uncertainty enough to make *optimal* therapeutic decisions.<sup>139</sup>

Of utmost relevance to regulatory interventions, a critical issue through the diagnostic process then is deciding *when* sufficient information has been obtained to make a reliable diagnosis.

Second, this shared decision-making context of “diagnostic indeterminacy” has inspired a common evaluative approach. Namely, much like the importance of political experience and judgment to formulating useful legislative

measures, “[a]ccurate, timely, and patient-centered diagnosis relies on proficiency of *clinical reasoning*”,<sup>140</sup> an evaluative process that involves the proper exercise of “judgment under uncertainty”.<sup>141</sup> Based “[...] within clinicians’ minds (facilitated or impeded [contextually] by the work system)”,<sup>142</sup> and influenced by “dual process theory” (i.e. a combination of analytical and non-analytical models), clinical reasoning has been defined by the National Academy of Sciences “[...] as the clinician’s *quintessential competency*”—being “the cognitive process that is necessary to evaluate and manage a patient’s medical problems”.<sup>143</sup>

Third, the conceptual model of medical diagnosis also demonstrates—not unlike *Murray* and *Sander*’s “systems-inspired” regulatory models—that the diagnostic process takes place within a complex, dynamic, and interrelated *context* (i.e. “work system”), consisting of: (1) diagnostic team members; (2) tasks; (3) technologies and tools; (4) organisational factors; (5) the physical environment; and (6) the external environment. As with “systems thinking” more generally, it is crucial to recall that—like *Murray*’s “complexity thesis” and the many levels of abstraction involved in *Engel*’s “biopsychosocial” model—this diagnostic “work system” provides the *inescapable* context within which evaluative decision-making occurs, meaning—perhaps, above all—that “[a]ll components of the work system *interact*, and [...] *affect* the diagnostic process [...]”.<sup>144</sup> In short, all is relational.

#### bb) Regulatory lessons: Indeterminate interventions in multi-ordinal environments

As seen from medical diagnostics’ three conceptual pillars, the parallels between the decision-making processes and requirements of clinical reasoning and “systems-based” online regulatory models are salient, pointing to several key lessons.

First, there exists a striking *similarity-of-structure* between *Murray*’s earlier regulatory proposals and the nature of diagnostic science. Despite his settled view of the indeterminacy of the online environment, *Murray*’s conviction of its malleability and amenability to regulation prompted endorsement of a “three-step” protocol remarkably like the diagnostic process. His self-reflexive stages of environmental mapping, regulatory interventions, and evaluation and incorporation of regulatory feedback essentially restate the three diagnostic stages of information gathering, integration and interpretation, and updating working hypotheses.

Second, as also forecasted by *Murray* and his “complexity thesis”—much like reframing health and illness within

a broader *biopsychosocial* framework—cyberspace must be similarly understood as a complex networked environment.<sup>145</sup> Besides *Murray*’s regulatory call for a “non-interventionist” approach,<sup>146</sup> the self-reflexive method driving medical diagnosis speaks (at the very least) to the fundamental procedural *necessity* of engaging in unbounded probing of potential aetiological (or regulatory) factors *well before* ending the investigative process. Freed from unnecessary ideological impediments and investigatory blind spots, “systems-inspired” regulatory approaches must take seriously a full panoply of potential causal/aetiological factors. In other words, before regulatory problems can be effectively “overcome”, all relevant factors must first be *tabled* for consideration.

Lastly, this commitment to minimally encumbered scientific investigation significantly amplifies the *structural* regulatory concerns of *Murray*, *Lavi*, and *Sander*. By incorporating the broader “work system” into the diagnostic process—and its implicit recognition of the *causal* influences of the “physical” and “external” environments—scientific inquiry is not only freed from “blind spots” compromising our diagnosis of hidden dysfunctions, but for crafting suitable prescriptions or “treatments”. Importantly, our comprehensive review of leading “systems thinking” models demonstrates that even together they exhibit insufficient attention to confirming the *systemic effects* and prescriptive implications of state regulations and content moderation practices on the overall health of our digital public sphere. Whether in regulatory or academic contexts, more work needs to be done. When considered in light of Canada’s proposed Online Harms Act, the relevantly overlooked “social and environmental signals” would appear to be the economic drivers of contemporary digital censorship (i.e. over-filtering and over-blocking), and the relationship between its “systems-based” transparency obligations and the rise of privatised government censorship—factors intuited by average Canadians, but not taken up satisfactorily by either of their expert advisors or political representatives.

## V. Conclusion

As we have seen, with the possible exception of *Murray*’s original “complexity thesis”, growing appeals to “systems-based” online regulatory approaches by legal commentators and regulators alike would appear to be at considerable risk of overpromising and underdelivering. It is more than ironic that whilst engaging in a comprehensive review of this burgeoning “second wave” of “systems-inspired” regulatory material, it remains difficult (if not impossible) to acquire a full complement of the “patterns and in-

terrelationships” that Canadian legislators initially seemed so desperate to acquire. Despite their individual contributions, what remains to be done—indeed, very much like acquiring missing pieces of “a bigger puzzle”—is incorporating each scholar’s theoretical contributions and insights into a broader, composite regulatory framework better suited to tracking the systemic effects of state and platform practices on the *overall* social media environment. A critical and largely ignored component of any genuine “systems-inspired” regulatory approach must be to embrace *systemic causation*.

This need for adopting a more integrative approach to online phenomena was also shown by profound insights native to social medicine and diagnostic theory. Besides providing a convincing case for expanding aetiological (and regulatory) inquiry to include the effects of social and environmental signals, established principles of medical diagnosis also provided a valuable decision-making protocol for online regulators. Here too, our extensive review of leading “systems-inspired” regulatory models indicates that the nearest we can expect to approximate the scientific neutrality and openness of the diagnostic method is to *combine* the contributions of leading scholars into a comprehensive system. Rather than supporting current regulatory preoccupations with harmful online content—as shown by Canada’s over-criminalisation of hate offences in its proposed Online Harms Act—early indications point to taking more seriously the underlying infrastructure and economic drivers not only of harmful content and disinformation, but of rising censorship and risks of over-regulating online speech interests.

The key takeaway from our review of “systems-inspired” regulatory scholarship and medico-diagnostic principles consequently is that prevailing “systems-based” regulatory

approaches—as epitomised by Canada’s new Online Harms Act—would appear to function as a “blueprint” for privatised government censorship, providing regulators with the legislative mandate, informational transparency, and compliance authority for regulatory capture that leading free speech scholars have appropriately labelled the “moderators’ dilemma”. That is to say, “the more speech-protective the government’s policy, the more *hands-on* the government’s approach will need to be”.<sup>147</sup> As shown by Canada’s newly proposed “systems-based risk-assessment” model, this unsettling trade-off “sewn into the logic of the Internet”, not only appears to apply to combating increasing online censorship by using “must-carry” legal interventions (i.e. common-carrier laws preventing the exclusion of speakers or restricting content), but to all regulatory “proxy-censor” interventions aimed at tamping down harmful online content.<sup>148</sup> Since Canadian regulators have not engaged in an uncompromising “differential diagnosis” of online phenomena—which, as we have seen, benefits diagnosticians and legislators alike by situating the patient’s or public sphere’s symptoms in their *broadest aetiological context*—we are tempted, perhaps ironically, to look not to the future, but to the distant past.

After all these years, *Virchow’s* pioneering view on the diagnosis and regulation of public health remains an invaluable perspective that Canada and other countries would do well to study and apply. In a dynamic, interconnected world increasingly at odds with the principle of territoriality—where “physicians are the natural attorneys of the poor”, and politicians its “natural anthropologists”—it is with some surprise and much regret that it remains a matter of any controversy or dismay that we lawyers and jurists should bear a greater share of the solemn responsibility of being its “natural diagnosticians”.

1 See generally M. McLuhan, *The Gutenberg Galaxy: The Making of Typographic Man*, 1962; M. McLuhan, *Understanding Media: Extensions of Man*, 1964. See also S. Grampp, *Marshall McLuhan: Eine Einführung*, 2011.

2 See R. Stephenson and J. Rinceanu, “Digital Iatrogenesis: Towards an Integrative Model of Internet Regulation”, (2023) 1 *eucri*, 73.

See generally L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, 2014; L. Floridi, “The End of an Era: from Self-Regulation to Hard Law for the Digital Industry”, (2021) 34 *Philosophy & Technology*, 619.

3 See e.g. E. B. Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility*, 2015, p. 15; H. Jenkins et al., *Confronting the Challenges of Participatory Culture: Media Education for the 21st Century*, 2006.

4 See e.g. G. M. Dickinson, “Big Tech’s Tightening Grip on Internet Speech”, (2022) 55 *Indiana Law Review*, 101; M. Moore and D. Tambini

(eds.), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*, 2018; K. Langvardt, “A New Deal for the Online Public Sphere”, (2018) 26 *George Mason Law Review*, 341, 381.

5 See R. J. Hamilton, “Governing the Global Public Square”, (2021) 62 *Harvard International Law Journal*, 117; J. Peters and B. Johnson, “Conceptualizing Private Governance in Networked Society”, (2016) 18 *North Carolina Journal of Law and Technology*, 15.

6 See J. Bayer, “Rights and Duties of Online Platforms”, in: J. Bayer et al. (eds.), *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe*, 2021; K. Klonick, “The New Governors: The People, Rules, and Processes Governing Online Speech”, (2018) 131 *Harvard Law Review*, 1598.

7 See U.S. Supreme Court, *Biden v Knight First Amendment Institute*, 141 S. Ct. 1220, 1221 (2021) (Thomas J., concurring).

8 See S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019; J. M. Balkin, “Old-



**Dr. Randall Stephenson, LL.M. (Columbia), M.St., D.Phil. (Oxon)**

Senior Researcher, Public Law Department, Max Planck Institute for the Study of Crime, Security and Law, Freiburg i.Br., Germany



**Dr. Johanna Rinceanu LL.M. (Washington, D.C.)**

Senior Researcher, Criminal Law Department, Max Planck Institute for the Study of Crime, Security and Law, Freiburg i.Br., Germany

School/New-School Speech Regulation”, (2014) 127 *Harvard Law Review*, 2296.

9 See Brief of Professor P. Hamburger as Amicus Curiae in Support of Neither Party, U.S. Supreme Court, 24 October 2022, *Ashley Moody, Attorney General of Florida et al. v. NetChoice, LLC et al.*, No. 22-277; J. M. Balkin, “Free Speech is a Triangle”, (2018) 118 *Columbia Law Review*, 2011.

10 R. Stephenson and J. Rinceanu, (2023) 1 *eu crim*, *op. cit.* (n. 2), 73, 73–74.

11 See Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) from 1 September 2017 (BGBl I p. 3352).

12 See R. Aiello, “Where Does the Liberal Promise to Address Harmful Online Content Stand?”, CTV News.ca, 30 August 2022, para. 2, available at <<https://www.ctvnews.ca/politics/where-does-the-liberal-promise-to-address-harmful-online-content-stand-1.6048720>> accessed 5 April 2024.

13 R. Aiello, *op. cit.* (n. 12), para. 17.

14 R. Aiello, *op. cit.* (n. 12), para. 13.

15 See e.g. Hamburger Brief, *op. cit.* (n. 9); S. Zuboff, *op. cit.* (n. 8); J. M. Balkin, (2014) 127 *Harvard Law Review*, *op. cit.* (n. 8), 2296; J. M. Balkin, “The First Amendment is an Information Policy”, (2012) 41 *Hofstra Law Review*, 1, 27–28 et seq., where the author provides a useful roadmap of “new school censorship”.

16 See e.g. K. Langvardt, “Regulating Online Content Moderation”, (2018) 106 *The Georgetown Law Journal*, 1353, 1363.

17 See e.g. R. Virchow, “Der Armenarzt”, (1848) 18 *Die Medicinische Reform*, 125.

18 NetzDG, *op. cit.* (n. 11); Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L1277/1. See also Online Safety Act 2023 (UK).

19 See J. Bayer, *op. cit.* (n. 6), p. 30.

20 See R. Stephenson and J. Rinceanu, (2023) 1 *eu crim*, *op. cit.* (n. 2), 73, 74.

21 See J. Bayer et al., “Conclusions: Regulatory Responses to Communication Platforms: Models and Limits”, in: J. Bayer et al. (eds.), *op. cit.* (n. 6), p. 571.

22 See J-M. Kamatali, “‘Hate Speech’ in America: Is it Really Protected?”, (2021) 61 *Washburn Law Journal*, 163; J-M. Kamatali, “The Limits of the First Amendment: Protecting American Citizens’ Free

Speech in the Era of the Internet & the Global Marketplace of Ideas”, (2015) 33 *Wisconsin International Law Journal*, 587.

23 See Department of Canadian Heritage, “What We Heard: The Government’s Proposed Approach to Address Harmful Content Online” (Government of Canada, 3 February 2022), Lack of Definitional Detail section, para. 2, available at <<https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/what-we-heard.html>> accessed 5 April 2024.

24 Department of Canadian Heritage, “What We Heard”, *op. cit.* (n. 23), Proactive Monitoring Obligation section, para. 1 (emphasis in original).

25 Department of Canadian Heritage, “What We Heard”, *op. cit.* (n. 23), 24-hour Inaccessibility Requirement section, para. 1.

26 Department of Canadian Heritage, “What We Heard”, *op. cit.* (n. 23), Alternative Approaches section, para. 1 (emphasis added).

27 Department of Canadian Heritage, “What We Heard”, *op. cit.* (n. 23), Alternative Approaches section, para. 1 (emphasis added).

28 Department of Canadian Heritage, “What We Heard”, *op. cit.* (n. 23), The Necessity of New Regulators section, para. 1.

29 Department of Canadian Heritage, “What We Heard”, *op. cit.* (n. 23), Transparency and Accountability Requirements section, para. 2.

30 See Department of Canadian Heritage, “The Government’s Commitment to Address Online Safety” (Government of Canada, 8 July 2022), p. 2 (emphasis added), available at <<https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html>> accessed 5 April 2024.

31 See Department of Canadian Heritage, “Introductory Session” (Government of Canada, 28 April 2022), Theme F: The Regulatory Toolkit section, para. 3, available at <<https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/introductory-session.html>> accessed 5 April 2024.

32 See Department of Canadian Heritage, “Summary of Session Two: Objects of Regulation” (Government of Canada, 28 April 2022), Takedown Requirements section, para. 2 (emphasis added), available at <<https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/session-two-summary.html>> accessed 5 April 2024.

33 See Department of Canadian Heritage, “Summary of Session Three: Legislative and Regulatory Obligations” (Government of Canada, 6 May 2022), Human Rights section, para. 4 (emphasis added), available at <<https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/summary-session-three.html>> accessed 5 April 2024; Department of Canadian Heritage, “Supplemental Worksheet: Legislative and Regulatory Obligations” (Government of Canada, 10 May 2022), General Monitoring Scheme section, para. 1 (emphasis added), available at <<https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/session-five-legislative-regulatory-obligations.html>> accessed 5 April 2024.

34 See Department of Canadian Heritage, “Summary of Session Six: Freedom of Expression and Other Rights” (Government of Canada, 27 May 2022), Theme A: Charter Rights section, para. 3, available at <<https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/summary-session-six.html>> accessed 5 April 2024.

35 See Department of Canadian Heritage, “Summary of Session Three”, *op. cit.* (n. 33), Theme A: Duties Imposed on Regulated Services section, para. 2.

36 Department of Canadian Heritage, “Summary of Session Three”, *op. cit.* (n. 33), Human Rights section, para. 3 (emphasis added).

37 See Department of Canadian Heritage, “Summary of Session Eight: Disinformation” (Government of Canada, 10 June 2022), Theme A: Understanding the Magnitude of the Challenge section, para. 5 (emphasis added), available at <<https://www.canada.ca/en/canadi>



[an-heritage/campaigns/harmful-online-content/summary-session-eight.html](#)> accessed 5 April 2024.

38 Department of Canadian Heritage, “Summary of Session Eight”, *op. cit.* (n. 37) (emphasis added).

39 Department of Canadian Heritage, “Summary of Session Eight”, *op. cit.* (n. 37), Theme C: Approaches to Addressing Disinformation and its Effects through a Risk-Based Approach section, para. 6.

40 3rd Canadian Citizens’ Assembly on Democratic Expression, “Citizens’ Assembly on Democratic Expression: Recommendations for Reducing Online Harms and Safeguarding Human Rights in Canada”, (Public Policy Forum, 2022), p. 5.

41 3rd Canadian Citizens’ Assembly on Democratic Expression, “Citizens’ Assembly on Democratic Expression”, *op. cit.* (n. 40), p. 10, p. 51 (emphasis added).

42 3rd Canadian Citizens’ Assembly on Democratic Expression, “Citizens’ Assembly on Democratic Expression”, *op. cit.* (n. 40), p. 10.

43 3rd Canadian Citizens’ Assembly on Democratic Expression, “Citizens’ Assembly on Democratic Expression”, *op. cit.* (n. 40), p. 49 (emphasis added).

44 See Department of Canadian Heritage, “What we Heard: 2022 Roundtables on Online Safety” (Government of Canada, 31 January 2023), available at <<https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/what-we-heard/report.html>> accessed 5 April 2024. The public consultation process effectively ended with consultations with Indigenous peoples in January 2023. See Department of Canadian Heritage, “What we Heard Report: Indigenous Online Safety” (Government of Canada, 2023) available at <<https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/what-we-heard-online-safety.html>> accessed 5 April 2024.

45 Department of Canadian Heritage, “What we Heard”, *op. cit.* (n. 44), Surrey, British Columbia section, para. 2.

46 Department of Canadian Heritage, “What we Heard”, *op. cit.* (n. 44), Charlottetown, Prince Edward Island section, para. 4, Saskatoon, Saskatchewan section, para. 4.

47 Bill C-63, An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts, 1st Sess., 44th Parl., 2021–2024 (first reading 26 February 2024).

48 Bill C-63, An Act to enact the Online Harms Act, *op. cit.* (n. 47), cl. 15 (Part 2: Criminal Code).

49 Bill C-63, An Act to enact the Online Harms Act, *op. cit.* (n. 47), cl. 34 (Part 3: Canadian Human Rights Act).

50 See M. L. Mueller, *Networks and States: The Global Politics of Internet Governance*, 2010, p. 9. See also L. DeNardis, *The Global War for Internet Governance*, 2014, p. 6, who rightly emphasises that Internet governance encompasses both its technological infrastructure and the substantive policies developed around both its limitations and possibilities.

51 See e.g. R. H. Weber, *Realizing a New Global Cyberspace Framework: Normative Foundations and Guiding Principles*, 2015, p. 1. See also G. Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability*, 2020, Part VII. For a pioneering article on Internet jurisdiction and the limits of the principle of territoriality, see M. Geist, “Is There a There There? Towards Greater Certainty for Internet Jurisdiction”, (2001) 16 *Berkeley Technology Law Journal*, 1345.

52 R. H. Weber, *op. cit.* (n. 51), p. 89 (emphasis added).

53 See A. D. Murray, *The Regulation of Cyberspace: Control in the Online Environment*, 2007.

54 A. D. Murray, *op. cit.* (n. 53), p. 54.

55 A. D. Murray, *op. cit.* (n. 53), p. 237 (emphasis in original).

56 A. D. Murray, *op. cit.* (n. 53), p. 244 (emphasis in original).

57 A. D. Murray, *op. cit.* (n. 53), p. 54, pp. 233–251.

58 A. D. Murray, *op. cit.* (n. 53), p. 234.

59 A. D. Murray, *op. cit.* (n. 53), p. 234.

60 A. D. Murray, *op. cit.* (n. 53), p. 53.

61 A. D. Murray, *op. cit.* (n. 53), p. 53.

62 A. D. Murray, *op. cit.* (n. 53), p. 250 (emphasis added).

63 A. D. Murray, *op. cit.* (n. 53), pp. 250–251.

64 A. D. Murray, *op. cit.* (n. 53), pp. 250–251.

65 A. D. Murray, *op. cit.* (n. 53), p. 250.

66 A. D. Murray, *op. cit.* (n. 53), p. 251.

67 See R. H. Weber, *op. cit.* (n. 51), p. 90; C. Reed, *Making Laws for Cyberspace*, 2012, p. 220. Reed preferred a “heuristic” regulatory approach based on more abstract “rules of thumb” (*Ibid.*, p. 221).

68 M. Lavi, “Content Providers’ Secondary Liability: A Social Network Perspective”, (2016) 26 *Fordham Intellectual Property Media & Entertainment Law Journal*, 855. See also S. B. Spencer, “The First Amendment and the Regulation of Speech Intermediaries”, (2022) 106 *Marquette Law Review*, 1.

69 M. Lavi, *op. cit.* (n. 68), 879.

70 M. Lavi, *op. cit.* (n. 68), 888 (emphasis added).

71 M. Lavi, *op. cit.* (n. 68), 909.

72 M. Lavi, *op. cit.* (n. 68), 930. Importantly, Lavi argued that “notice-and-takedown” regimes are superior to negligence models in that the latter often result in legal ambiguity that has a disproportionate “chilling effect” on content moderation (*Ibid.*).

73 M. Lavi, *op. cit.* (n. 68), 910 (emphasis added).

74 M. Lavi, *op. cit.* (n. 68), 879, n. 117 cites J. M. Balkin, (2014) 127 *Harvard Law Review*, *op. cit.* (n. 8), 2296. See also J. M. Balkin, “How to Regulate (and Not Regulate) Social Media”, (2021) 1 *Journal of Free Speech Law*, 71; J. M. Balkin, (2018) 118 *Columbia Law Review*, *op. cit.* (n. 9), 2011.

75 M. Lavi, (2016) 26 *Fordham Intellectual Property Media & Entertainment Law Journal*, *op. cit.* (n. 68), 855, 936–937 (emphasis added).

76 See Hamburger Brief, *op. cit.* (n. 9).

77 See generally R. Stephenson, *A Crisis of Democratic Accountability: Public Libel Law and the Checking Function of the Press*, 2018.

78 See B. Sander, “Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law”, (2021) 32 *European Journal of International Law*, 159.

79 B. Sander, *op. cit.* (n. 78), 192 (emphasis added).

80 B. Sander, *op. cit.* (n. 78), 192 (emphasis added).

81 B. Sander, *op. cit.* (n. 78), 160.

82 B. Sander, *op. cit.* (n. 78), 162.

83 B. Sander, *op. cit.* (n. 78), 162.

84 B. Sander, *op. cit.* (n. 78), 162.

85 B. Sander, *op. cit.* (n. 78), 162 (emphasis added), citing E. Douek, “Governing Online Speech: From ‘Posts-as-Trumps’ to Proportionality and Probability”, (2021) 121 *Columbia Law Review*, 759.

86 B. Sander, (2021) 32 *European Journal of International Law*, *op. cit.* (n. 78), 159, 162 (emphasis added).

87 See also B. Dvoskin, “Expert Governance of Online Speech”,

(2023) 64 *Harvard International Law Journal*, 85; S. Marks, “Human Rights and Root Causes”, (2011) 74 *Modern Law Review*, 57.

88 B. Sander, (2021) 32 *European Journal of International Law*, *op. cit.* (n. 78), 159, 163.

89 See e.g. E. Volokh, “Treating Social Media Platforms like Common Carriers?”, (2021) 1 *Journal of Free Speech Law*, 377; G. Lakier, “The Non-First Amendment Law of Freedom of Speech”, (2021) 134 *Harvard Law Review*, 2299, 2316–2331; J. M. Balkin, (2021) 1 *Journal of Free Speech Law*, *op. cit.* (n. 74), 71, 86–87.

90 E. Douek, “Content Moderation as Systems Thinking”, (2022) 136 *Harvard Law Review*, 526. See also O. Pollicino and E. Bietti, “Truth



- and Deception across the Atlantic: A Roadmap of Disinformation in the US and Europe”, (2019) 11 *Italian Journal of Public Law*, 43.
- 91 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 526, 528, 538.
- 92 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 532.
- 93 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 530 (emphasis added).
- 94 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 606.
- 95 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 606 (emphasis added).
- 96 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 530, 532.
- 97 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 605.
- 98 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 532.
- 99 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 586.
- 100 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), (emphasis added), citing L. M. Khan, “The Separation of Powers and Commerce”, (2019) 119 *Columbia Law Review*, 973, 980.
- 101 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 589.
- 102 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 591 (emphasis added).
- 103 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 592.
- 104 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 593.
- 105 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 595 (emphasis added).
- 106 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 594.
- 107 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 593–600.
- 108 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 595.
- 109 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 596.
- 110 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 597.
- 111 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 597–598.
- 112 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 600.
- 113 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 601.
- 114 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 601.
- 115 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 601.
- 116 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 602.
- 117 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 602 (emphasis added).
- 118 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 604.
- 119 See e.g. R. J. Hamilton, (2021) 62 *Harvard International Law Journal*, *op. cit.* (n. 5), 117, 162, who argues that digital media regulation minimises key dynamics worldwide—particularly in the Global South—necessitating a flexible regulatory template based on “locally contextualised” content moderation rules.
- 120 On systems theory, see e.g. N. Luhmann, *Introduction to Systems Theory*, 2013; G. Bateson, *Steps to an Ecology of Mind: Collected Essays in Anthropology, Psychiatry, Evolution, and Epistemology*, 1972; E. Laszlo (ed.), *The Relevance of General Systems Theory*, 1972; and L. von Bertalanffy, *General Systems Theory: Foundations, Development, Applications*, 1968. On accountability scholarship, see e.g. M. Bovens et al. (eds.), *The Oxford Handbook of Public Accountability*, 2014; M. Bovens, “Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism”, (2010) 33(5) *West European Politics*, 946; M. Bovens, “Analysing and Assessing Accountability: A Conceptual Framework”, (2007) 13(4) *European Law Journal*, 447; and R. Mulgan, *Holding Power to Account: Accountability in Modern Democracies*, 2003. See also K. Klonick, “Of Systems Thinking and Straw Men”, (2023) 136 *Harvard Law Review Forum*, 139, where the author critiques Douek’s misuse of the term “systems thinking”, and points out the importance of engaging with the discipline’s foundational literature.
- 121 E. Douek, (2022) 136 *Harvard Law Review*, *op. cit.* (n. 90), 526, 586 (emphasis added).
- 122 See R. Stephenson and J. Rinceanu, (2023) 1 *eucri*, *op. cit.* (n. 2), 73.
- 123 R. Stephenson and J. Rinceanu, (2023) 1 *eucri*, *op. cit.* (n. 2), 73, 78.
- 124 See B. Cardozo, “Anniversary Discourse: What Medicine Can do for Law”, (1929) 5 *Bulletin of the New York Academy of Medicine*, 581, 584 (emphasis added).
- 125 R. Virchow, *Gesammelte Abhandlungen aus dem Gebiete der Öffentlichen Medicin und der Seuchenlehre*, Erster Band, 1879, p. 121.
- 126 R. Virchow, (1848) 18 *Die Medicinische Reform*, *op. cit.* (n. 17), 125, 125 (emphasis added).
- 127 R. Virchow, “Was die ‘medizinische Reform’ will”, (1848) 1 *Die Medicinische Reform*, 2 (emphasis added).
- 128 R. Virchow, *Disease, Life and Man: Selected Essays by Rudolf Virchow*, Lelland J. Rather (trn.), 1958, p. 66 (emphasis added).
- 129 See R. Koch, “Die Aetiologie der Tuberkulose”, (1882) 15 *Berliner Klinische Wochenschrift*, 221.
- 130 See G. L. Engel, “A Unified Concept of Health and Disease”, (1960) 3 *Perspectives in Biology and Medicine*, 459; G. L. Engel, “The Need for a New Medical Model: A Challenge for Biomedicine”, (1977) 196 *Science*, 129.
- 131 See G. L. Engel, “Misapplication of a Scientific Paradigm”, (1985) 3 *Integrative Psychiatry*, 9.
- 132 G. L. Engel, (1960) 3 *Perspectives in Biology and Medicine*, *op. cit.* (n. 130), 459, 485 (emphasis added).
- 133 R. Virchow, (1848) 1 *Die Medicinische Reform*, *op. cit.* (n. 127), 2, 2.
- 134 See e.g. R. C. Strohmman, “Ancient Genomes, Wise Bodies, Unhealthy People: Limits of a Genetic Paradigm in Biology and Medicine”, (1993) 37 *Perspectives in Biology and Medicine*, 112.
- 135 T. Kuhn, *The Structure of Scientific Revolutions*, 2nd ed., 1970.
- 136 See E. P. Balogh et al. (eds.), *Improving Diagnosis in Health Care*, 2015, p. 31.
- 137 E. P. Balogh et al., *op. cit.* (n. 136), p. 32.
- 138 E. P. Balogh et al., *op. cit.* (n. 136), p. 34.
- 139 E. P. Balogh et al., *op. cit.* (n. 136), pp. 48–49 (emphasis added).
- 140 E. P. Balogh et al., *op. cit.* (n. 136), p. 53 (emphasis added).
- 141 E. P. Balogh et al., *op. cit.* (n. 136), p. 53 (emphasis added).
- 142 E. P. Balogh et al., *op. cit.* (n. 136), p. 53 (emphasis added).
- 143 E. P. Balogh et al., *op. cit.* (n. 136), p. 53 (emphasis added).
- 144 E. P. Balogh et al., *op. cit.* (n. 136), p. 34 (emphasis added).
- 145 See generally Y. Benkler, “A Free Irresponsible Press: Wikileaks and the Battle Over the Soul of the Networked Fourth Estate”, (2011) 46 *Harvard Civil Rights-Civil Liberties Law Review*, 311; Y. Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, 2006.
- 146 A. D. Murray, *op. cit.* (n. 53), p. 54.
- 147 K. Langvardt, (2018) 106 *The Georgetown Law Journal*, *op. cit.* (n. 16), 1353, 1363 (emphasis added).
- 148 See S. B. Spencer, (2021) 32 *European Journal of International Law*, *op. cit.* (n. 78), 9, where the author stressed that both regulatory forms differ significantly in their structural effects on “the total amount of speech” reaching the public sphere, viz., that “proxy-censor regulations *limit* the amount of speech in circulation, whereas must-carry regulations *increase* the amount of speech [...]” (emphasis added).

# 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](mailto:public-law@csl.mpg.de)



Internet: <https://csl.mpg.de>

Official Registration Number: VR 13378 Nz  
(Amtsgericht Berlin Charlottenburg)  
VAT Number: DE 129517720

**Editor in Chief:** Prof. Dr. Dr. h.c. mult. Ulrich Sieber

**Managing Editor:** Thomas Wahl, Max Planck Institute for the  
Study of Crime, Security and Law, Freiburg

**Editors:** Dr. András Csúri, Vienna University of Economics  
and Business; Dr. Anna Pinggen, Max Planck Institute for the  
Study of Crime, Security and Law, Freiburg; Cornelia Riehle,  
ERA, Trier

**Editorial Board:** Prof. Dr. Lorena Bachmaier, Complutense  
University Madrid, Spain; Peter Csonka, Head of Unit, DG Jus-  
tice and Consumers, European Commission Belgium; Prof.  
Dr. Esther Herlin-Karnell, University of Gothenburg, Sweden;  
Mirjana Juric, Head of Service for combating irregularities  
and fraud, Ministry of Finance, Croatia; Philippe de Koster,  
Director FIU Belgium; Prof. Dr. Katalin Ligeti, University of  
Luxembourg; Dr. Lothar Kuhl, Head of Unit, DG REGIO, Euro-  
pean Commission, Belgium; Prof. Dr. Ralf Poscher, Director  
at the Max Planck Institute for the Study of Crime, Security  
and Law, Freiburg, Germany; Lorenzo Salazar, Deputy Pro-  
secutor General to the Court of Appeal of Naples, 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, Secu-  
rity 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

© Max Planck Institute for the Study of Crime, Security and  
Law, 2024. All rights reserved: no part of this publication may  
be reproduced, stored in a retrieval system, or transmitted in any  
form or by any means, electronic, mechanical photocopying,  
recording, or otherwise without the prior written permission of  
the publishers.

Views and opinions expressed in the material contained in  
eucrim are those of the author(s) only and do not necessarily  
reflect those of the editors, the editorial board, the publisher,  
the European Union, the European Commission, or other con-  
tributors. Sole responsibility lies with the author of the contri-  
bution. The publisher and the European Commission are not  
responsible for any use that may be made of the information  
contained therein.

ISSN: 1862-6947

### Practical Information

Articles in eucrim are subject to an editorial review. The jour-  
nal is published four times per year and distributed electroni-  
cally for free.

In order to receive issues of the periodical on a regular basis,  
please write an e-mail to:

[eucrim-subscribe@csl.mpg.de](mailto:eucrim-subscribe@csl.mpg.de)

For cancellations of the subscription, please write an e-mail to:

[eucrim-unsubscribe@csl.mpg.de](mailto: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](mailto:info@eucrim.eu)



**MAX PLANCK INSTITUTE**  
FOR THE STUDY OF  
CRIME, SECURITY AND LAW

